White paper

6 steps to GDPR compliant email marketing

How can Spotler help with GDPR?

spotler

The General Data Protection Regulation will come into effect on the 25th of May 2018. This new regulation replaces the Dutch Personal Data Protection Act and will apply for the entire European Union. Possibly you might have already come across its abbreviation: GDPR, which stands for General Data Protection Regulation.
The GDPR has two major consequences:

- Stricter and expanded privacy rights.
- Extended responsibilities and obligations for organisations.

This means you will have to make a couple of changes to your email marketing process. To give you a head start, we have arranged these changes in the following six steps:

1. Mapping out which GDPR measures you need to take
2. Entering into a data processing agreement
3. Know which personal data you are collecting
4. Ensure the privacy rights of data subject
5. Know Spotler's safety measures
6. Adjust your privacy statement

Spotler will guide you through each step. We will even release a special GDPR software update in January of 2018 for our MailPlus software. This way you will have all the information you need to make sure your email marketing is GDPR compliant, stored in one place in your MailPlus account.

Good luck implementing the necessary measures.

Spotler

December 2017

INTRO

How does GDPR affect email marketing?

The GDPR regulates the protection of personal data. The word 'email' is not directly mentioned in the act. In the Netherlands the laws and regulations concerning email marketing have been successfully regulated for many years by the Telecommunications Act. The introduction of the GDPR will not change this.

As a marketer, however, you do collect and process personal data when applying email marketing techniques. At the least you are collecting email addresses and probably some other personal data as well. Processing this type of data is regulated by the GDPR.

Email marketing means data processing

According to the GDPR, all data that can identify a person, directly or indirectly, are considered personal data. Furthermore, the GDPR states that all the actions you perform with this data are considered data processing. Even deleting a record is considered data processing. This means that as an email marketer you are in fact processing personal data.

When is processing data for email marketing allowed?

The GDPR states that the processing of personal data is permitted if at least one of the following legal grounds is met:

1. Processing is necessary for the performance of a contract
2. The data subject has given explicit consent
3. There is a legitimate interest for processing the data
4. Processing is necessary to protect the vital interests of the data subject
5. There is a public interest for processing the data
6. It is necessary for compliance with a legal obligation

Email marketing is a form of direct marketing. The GDPR states the following about direct marketing in Recital 47:

'The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

This means the GDPR states that processing personal data for email marketing purposes is permitted based on the legitimate base regarding a legitimate interest. It is not necessary to ask for consent to process personal data for email marketing purposes.

Example: you have asked your clients or prospects for their date of birth so you can send them a nice birthday email. For this marketing action you will not need specific consent. Clients often appreciate these types of emails and will not consider it a violation of their privacy.

You could safely say that there is a legitimate interest involved. But be aware that according to the Telecommunications Act you should receive consent (opt-in) from your clients or prospects to be allowed to send them emails.

Can I keep sending emails to contacts in my current database after the 25th of May 2018?

Yes. It remains important that you only send commercial emails after receiving consent from your contacts. This consent is called opt-in. If you have already received their consent you will not have to ask them again.

The regulations regarding the opt-in are not stated in the GDPR but can be found in the Telecommunications Act and will still apply after the 25th of May 2018.

1

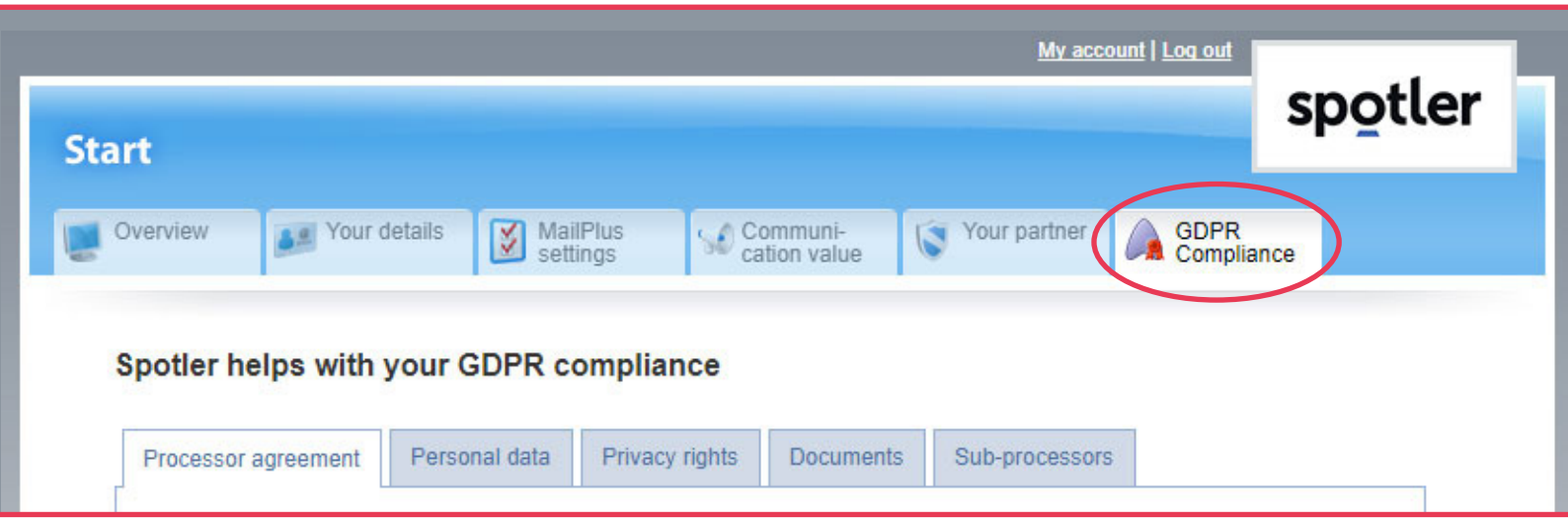
Mapping out which GDPR measures you need to take

As an organisation you have to be able to prove your GDPR compliancy. An important principle of the GDPR is transparency. It should be clear how you have implemented GDPR measures throughout your organisation, including your email marketing activities.

From January 2018, MailPlus will be expanded with an extra 'GDPR-compliance' tab where all the measures can be viewed directly. You can find all the data neatly presented in your own MailPlus account. This way Spotler solves an important piece of your GDPR compliancy puzzle for you.

How does Spotler help?

In January 2018 you will see the tab "GDPR-compliance" appear in the start menu of our software.



To comply with GDPR it is important to enter into a data processing agreement with us, to have a complete overview of personal data that you are processing, ensure the rights of subjects involved and to be able to prove you have taken the appropriate technical and organisational security measures. In the following chapters of this white paper we will provide you with more information about this topic, but it is good to know that you can also find all your GDPR compliancy obligations listed in a single place in your MailPlus account.

This way Spotler helps you to prove that your email marketing is compliant with GDPR in a transparent and orderly way.

What should you pay attention to?

Are you Spotler's client and are you using MailPlus? Then you are meeting all of your obligations. All GDPR compliancy measures, concerning your email marketing, will be met from January 2018.

Attention: naturally this only applies to the personal data that are stored within our software.

If you are processing personal data in other systems (CRM, HRM, administration or e-commerce software), you are obligated to implement the necessary GDPR measures for these systems as well.

You should be wary of and continuously keep checking if the personal data collected in our software are still being used (data minimisation).

From time to time you should also think about the purpose for which you are processing certain personal data and the relevancy of that purpose. These matters always require human effort, even if you use our software.

2

Enter into a data processing agreement

As Spotler's client, according to GDPR, you have the role of controller and Spotler the role of processor. As soon as your organisation hires a processor, it is mandatory for you to sign a processing agreement with them.

This means that you have to sign this type of agreement with Spotler. But not only that. If personal data acquired by a third party are added to MailPlus, a data processing agreement with the third party is also necessary.

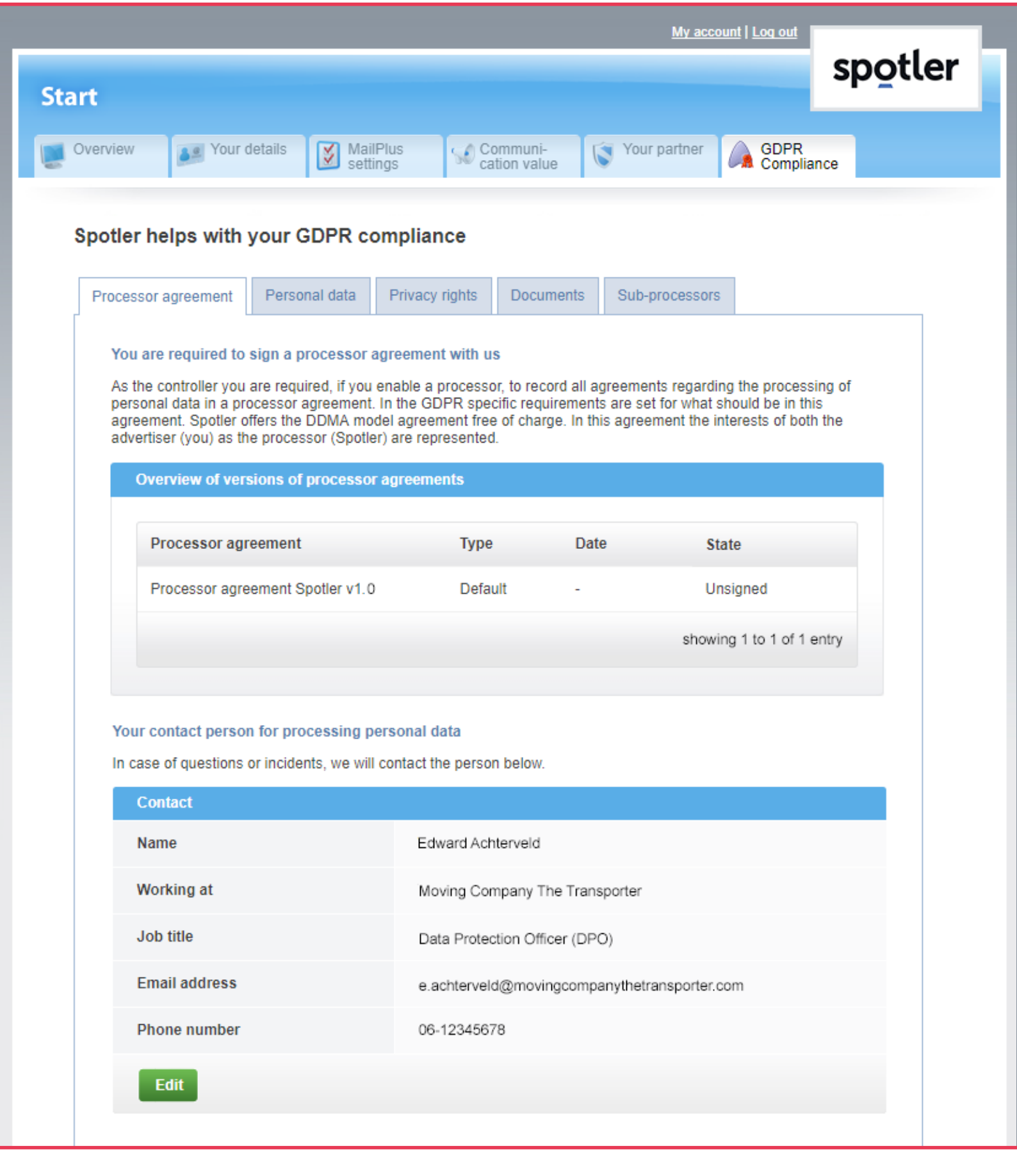
How does Spotler help?

The GDPR explicitly set the content of the data processing agreement.

For example: how the subjects' data will be used and for which purpose, indicating that the processor owns responsibility for all technical and organisational security measures, indicating that the processor assists with reporting security breaches.

Fortunately, the industry organisation DDMA (or Data Driven Marketing Association) has made a standard processing agreement available that is GDPR proof. Spotler offers you this agreement free of charge.

From January 2018, you can find this agreement on the special GDPR-page:



What should you pay attention to?

Conclude a data processing agreement with us
We advise you to sign the standard agreement that is available directly in our software. This way you are GDPR compliant and you can always choose to have a cus tom contract made afterwards.

You are by all means free to enter into a customised agreement with us, however, we would have to charge the time spent checking the GDPR compliancy of the customised agreement.

Evaluate the relationships with your partners
Anyone who has access to MailPlus must enter into a data processing agreement with Spotler. It does not matter if that person is you or someone of your email marketing associates. As soon as someone has access to personal data in MailPlus a data processing agreement is mandatory. This also includes all of Spotler's associates.

There are however two exceptions:

1. You have access to a subaccount of the MailPlus Franchise or MailPlus Corporate and your main office already has entered into an adequate data processing agreement.

2. You are not logging into MailPlus, but you have a (full service) associate working for you.

Remember: if you work with an associate, you should enter into a data processing agreement with them. Spotler cannot arrange this for you. You will have to contact your e-mail marketing associate and arrange this yourself.

Check your MailPlus integrations
Have you integrated MailPlus with your CRM-system or your online store? Make sure to check the nature of this connection. There are three ways MailPlus can be integrated and in one case you are obligated to enter into a data processing agreement with the party that facilitates this integration. To explain it:

If the data is directly synced to MailPlus from another software package there is no further action required. Another possibility is that the software is linked through our Connector Platform. In this case again you will not have to enter into an additional agreement, because this falls under the scope of our service.

If the software link is provided and hosted by a third party, you have to enter into another data processing agreement with them. In this case the personal data added to MailPlus is entered through a third party software, GDPR states that in this case there is another data processor involved.

Are you unsure if your software is linked with MailPlus trough a third party software? Contact us! We will gladly help you become GDPR compliant.

3

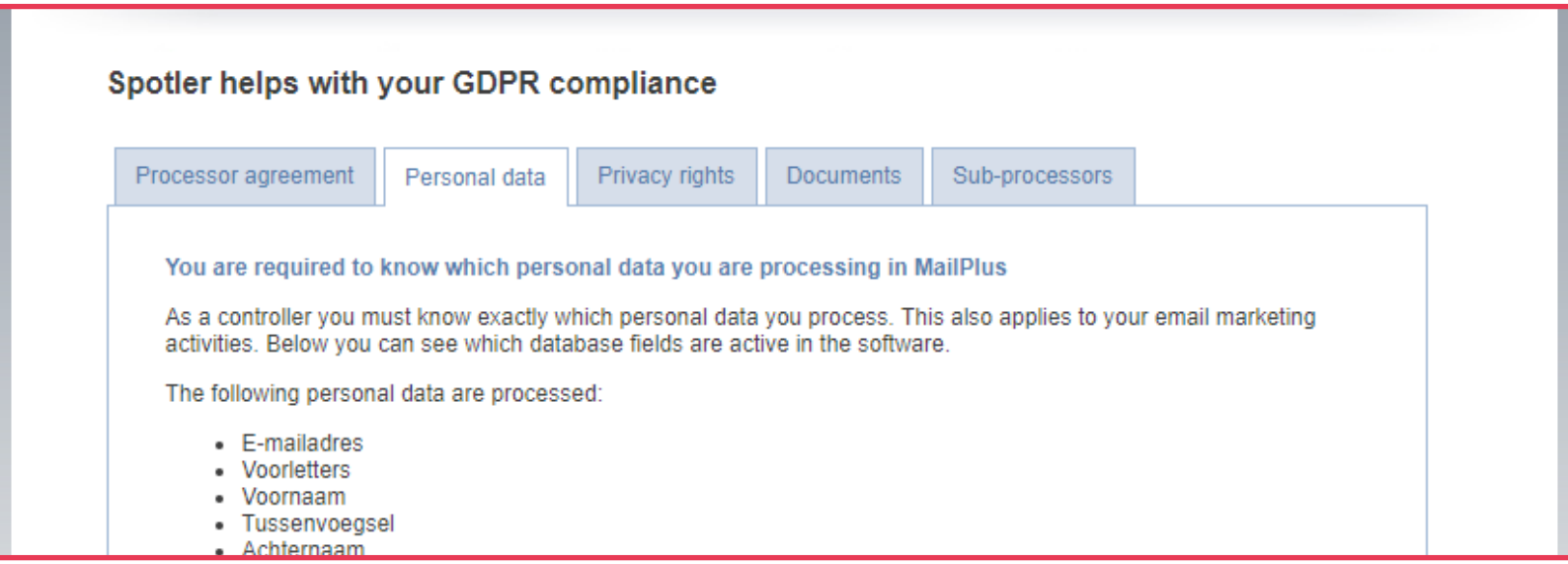
Know which personal data you are collecting

The GDPR obligates you to document which types of personal data you are processing for your email marketing activities and for which purpose you are doing so. In addition, you have the obligation to comply with data minimization.

You cannot store in your MailPlus account the personal data that you are not using for your email marketing activities. This means that you must know what personal data you are collecting and for what purpose.

How does Spotler help?

From January 2018 you will be able to see which personal data you are using for your email marketing activities on the GDPR-page:



This way Spotler has ensured that an important part of your GDPR compliancy is automatically regulated from within the software.

What should you pay attention to?

Make sure that you are actually using all the data that you are collecting for your email marketing activities. Be critical about the data you are not using, so either use them or remove them from MailPlus in order to be compliant with data minimisation.

Do not store any sensitive personal data
Spotler strongly advices against storing any sensitive personal data in our software. Apart from the fact that you need specific consent from the subject to process these data, they pose a high risk of harmful consequences for all parties involved. This type of data is referred to in the GDPR as special category personal data. For example: medical data, citizen service numbers, information about someone's identity, etc.

Technically, we cannot prevent you from storing sensitive personal data, because they are not within our control, but we strongly advice against storing this type of personal data.

Profile enrichment and segmentation will remain possible
Your usual email marketing activities remain possible under the GDPR, because they fall under the legitimate purpose of email marketing. It is fine to track open and clicking behaviour of your contacts, apply profile enrichment (implicit by behaviour and explicit by the recipient himself) and use these data for segmentation. Your email recipients will not mind these activities as most people enjoy receiving personalized emails.

The GDPR, however, is strict when it comes to automated decision making that is not beneficial to the receiver. For example, an insurance company is not permitted to automatically increase the premium if it seems that a client has an unhealthy lifestyle based on their purchase and clicking behaviour. Also, an online store may not automatically increase its prices if the IP address from a visitor comes from a high income neighbourhood.

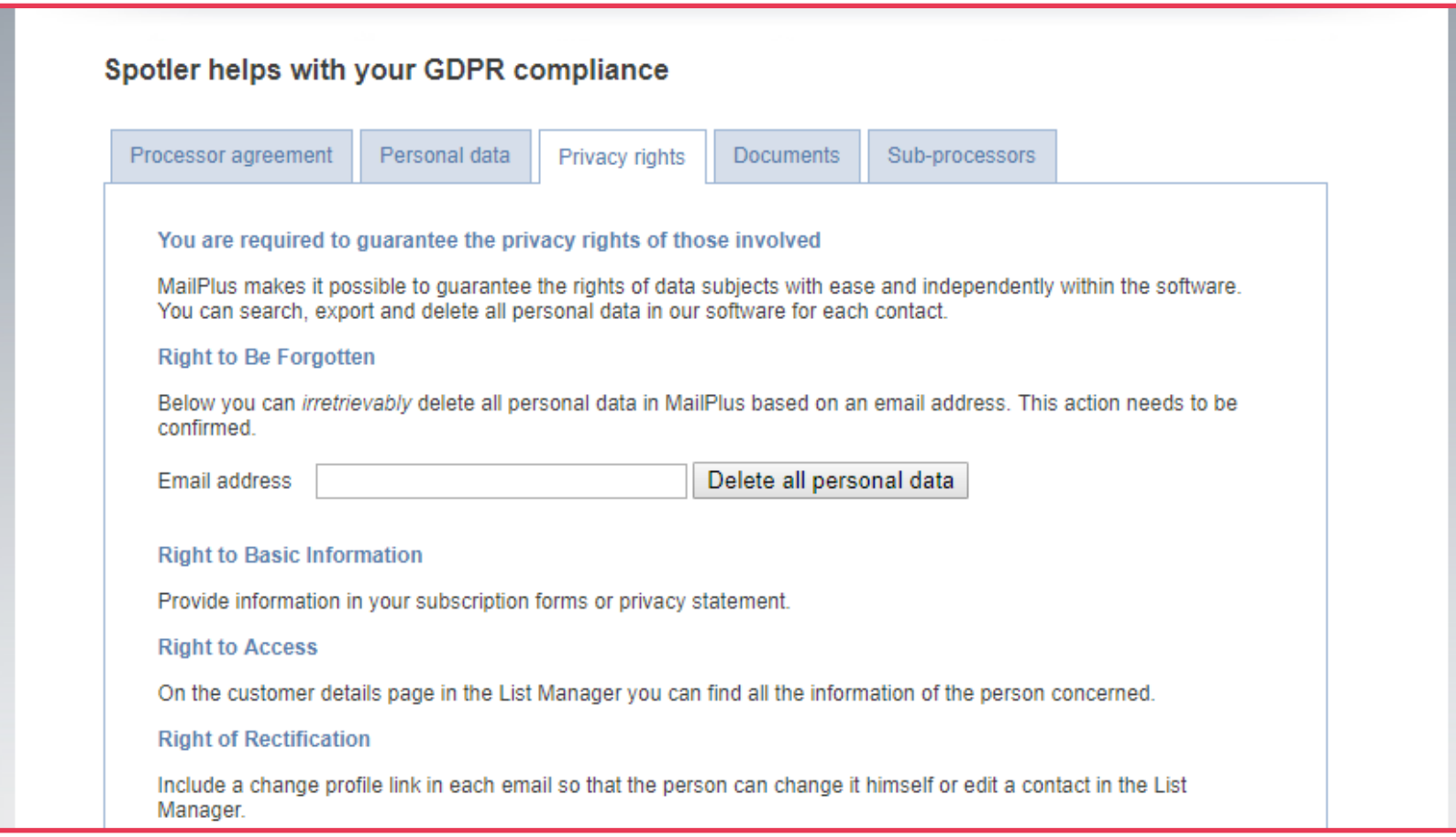
4

Ensure the privacy rights of data subjects

Each person added to your database has privacy rights. An consequence of GDPR is that these rights are reinforced and extended. You, as a data controller, are for that reason obligated to ensure that these rights are met. This includes the right of access, right to rectification, right to erasure and the right to data portability.

How does Spotler help?

If a person contacts your organisation and wants to exercise one of these rights, you have the obligation to comply. From January 2018 you can easily be of assistance to this person by going to the *Privacy Rights tab* on the GDPR-page.



The right to erasure is a new concept introduced by the GDPR. This means all personal data must be completely erased, as if the person has never existed in the database. We have made this possible within our software.

Attention: this action cannot be undone! In addition, in many cases MailPlus will not be the only system where personal data from this individual are stored.

What should you pay attention to?

All MailPlus users will be compliant with this GDPR obligation from January 2018. Ensuring the rights of your data subjects (for email marketing purposes) can be checked in your GDPR to-do list. Further actions are not necessary. What you should be mindful of is Retargeting.

Be careful about retargeting
The European Union wants to ensure enhanced digital protection and enhanced privacy rights for their citizens. Companies and organisations are forced to facilitate this. Many email marketers are wondering if they are allowed to retarget their email list and if they need additional data processing agreements to do so. The answer is 'yes' to both questions, but be mindful.

You are not allowed to share personal data with third parties without a subject's permission and you are obligated to enter into a data processing agreement with the third party.

Example: you would like to use Facebook Custom Audiences or Look-a-like Audiences. You share your email list with Facebook to display targeted adds on the time-line of a specific target audience. The GDPR specifies that you need the subject's permission to share their email address and you would be obligated to enter into a data processing agreement with Facebook.

The Dutch Consumers Association has recently approached 17 different companies about their Facebook Retargeting behaviour. These organisations did not ask for specific consent to share personal data with Facebook. Doing so is also prohibited by the Dutch Data Protection Act and it will certainly not be allowed under the GDPR. It is still unsure how the Dutch Personal Data Protection Authority will handle these cases. This should become more clear Iin the upcoming months.

DUTCH DATA PROTECTION AUTHORITY

What is the Dutch Data Protection Authority?

The Dutch Data Protection Authority (DPA) is the supervisory authority. It supervises the compliance with laws regarding the protection of personal data, both currently under the Dutch Data Protection Act and in the future under the GDPR. The DPA does this by conducting research, testing codes of conduct and by handling complaints.

5

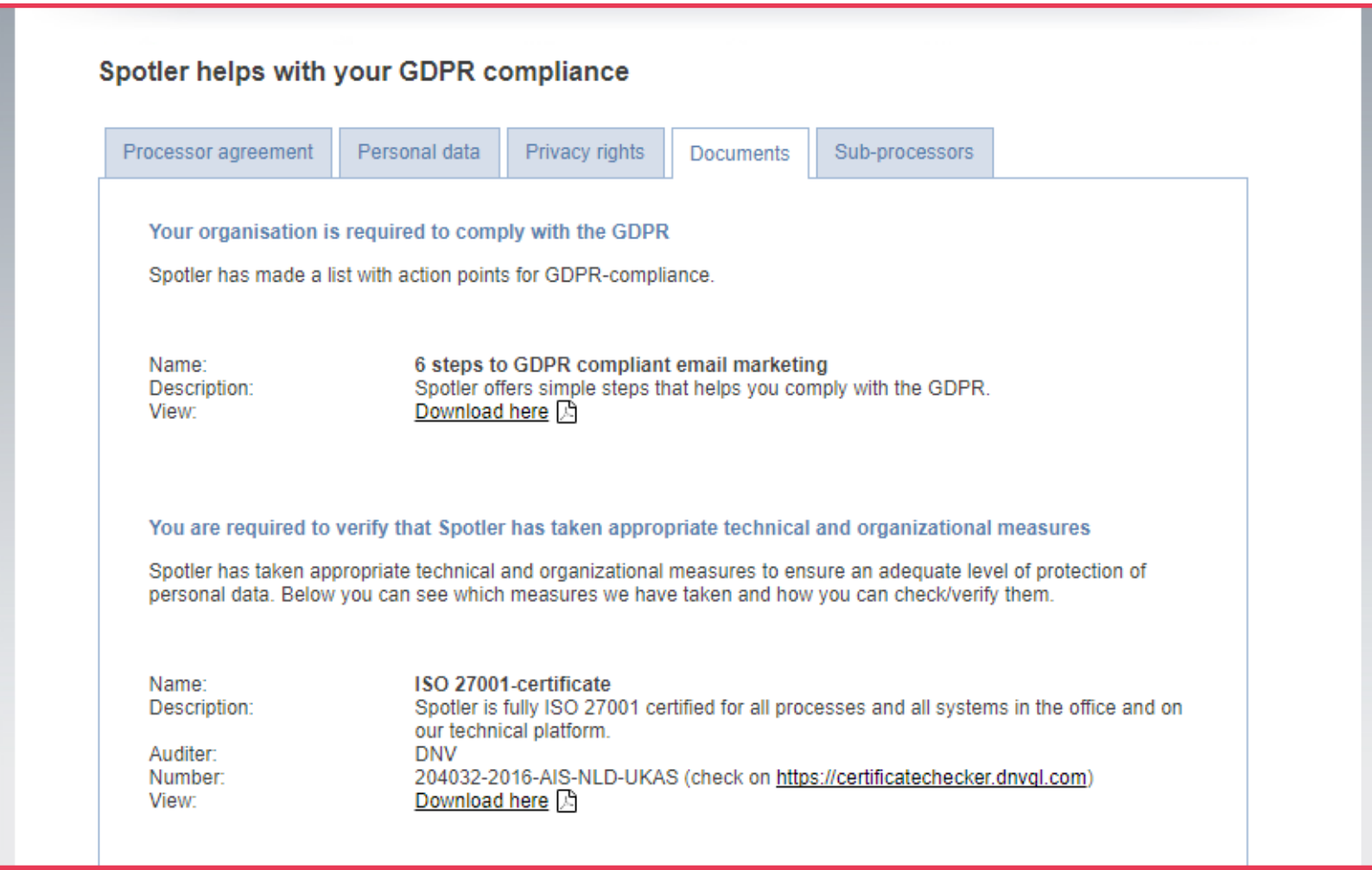
Know Spotler's security measures

In accordance with the GDPR, Spotler - as a processor- is obligated to take appropriate technical and organisational security measures that ensure the security of personal data stored in MailPlus. You, as controller, are obligated to evaluate if Spotler is meeting its obligations.

Unsurprisingly: we would like to assist you with this. Data security is a crucial part of Spotler's operational management.

How does Spotler help?

From January 2018 you can find the *Documents ta*b on the GDPR-page in our software:



The *Documents tab* contains important documents that will help you prove that Spotler is taking sufficient technical and organisational security measures. A listing of the documents:

ISO/IEC 27001:2013

ISO 27001 certification
Spotler is completely ISO 27001 certified for all processes and all systems in our office and on our technical platform. You can view our certificate in your MailPlus-account. You can review the validity and the scope of our certificate on the website of the auditor company DNV GL.

PRIVACY WAARBORG

DDMA privacy guarante
Not only is Spotler completely ISO 27001 certified, we have also received the DDMA privacy guarantee. With this guarantee, Spotler can assure you that we are using personal data in a careful and transparent manner, and that we meet all the necessary security measures.

Data Protection Officer
Spotler has an appointed Data Protection Officer (DPO). Our DPO oversees our compliance with and application of the Data Protection Act and from 25 may 2018 of the GDPR.

Keeping data within the European Economic Area (EEA)
The GDPR requires that all personal data are stored within the European Economic Area (EEA). The EEA includes all EU countries and Liechtenstein, Norway and Iceland. Spotler stores all its data in Amsterdam to meet this GDPR requirement.

All software and infrastructure is managed in-house
Not only do we store our data in the Netherlands, we also manage in-house our software and infrastructures which are used to store the data.

Spotler employees have no access to personal data
Spotler's employees do not have access to personal data without your specific consent. More information about this important measure, including how you can give your consent and under which terms, can be found under the *GDPR Compliancy tab*.

Two-step verification and secure file exchange
You can enable two-step verification to secure your access to MailPlus. Secure file exchange can also be enabled. More information on how you can enable these security measures can be found in the documents that will be available from January 2018, under the Documents tab inside the GDPR page.

What should you pay attention to?

You should be aware of the fact that you are required to report data breaches. With all the technical and organisational security measures in place, the chances that a security breach occurs are small. But should it happen, you are obligated to report this to the Dutch DPA.

Should a data breach occur, someone from the Spotler Management Team (MT) will contact you. In conformity with ISO 27001, we register all security incidents. In case of a major security breach – as a data breach – a protocol is started where our MT will be involved directly. On the GDPR-page in your MailPlus account you can view to which person inside your organisation we will report the data breach, and you can edit this if necessary

Is the Telecommunications Act still in effect after 25th of May 2018?

Certainly. Consumers will still need to give permission (opt-in) for receiving commercial mailings. The Data Protection Act or the GDPR do not require this, but it is mandatory under the Telecommunications Act.

This law prescribes that you should be able to prove opt-ins, but it fails to indicate how this should be done.

The new ePrivacy Regulation will replace the current Telecommunications Act, although its uncertain when it will happen exactly.

What about the ePrivacy Regulation?

Besides the GDPR, another relevant European law will possibly come into effect on the 25th May 2018: the ePrivacy Regulation.

This new law will replace the current Telecommunications Act. However, it is not very likely that this new law will take effect on the 25th of May 2018. Many European countries have submitted amendments to this new law. Spotler is keeping a close eye on the progress of the ePrivacy Regulation and will inform you timely when there are any new developments.

6

Adjust your privacy statement

The GDPR does not mention specifically what should be included in your privacy statement. However, it is wise to think it through.

The GDPR's core values are transparency and clear communication about storing and using personal data. This is why we advise you to review your privacy statement and edit it if necessary.

How does Spotler help?

MailPlus automatically tracks people's interactions, such as, for example, the open and click behaviour of an individual who has received a mailing. The GDPR requires that you should be transparent about all use of personal data. This is why we advise you to make a mention of this in your privacy statement, including the purpose for which you are using the data. Below is a suggestion on how to do this:

In case you are receiving our emails, we will track your interaction to them, with *the purpose of personalizing the content of our communications to better suit your interests.*

What should you pay attention to?

Your Privacy Statement is eminently the best place to be transparent about the way you are processing personal data. Not only for your email marketing, but for all of your services and communications.

Check if you are transparent about the cookies that you are using on your website and inform people on how they can file a privacy complaint.

Disclaimer

Spotler has paid the utmost care to the correctness and reliability of this white paper. Despite the time and care we spent preparing this whitepaper, it is possible, partly due to the choices made in the interpretation of the GDPR, that it contains some inaccuracies or incompleteness. For this reason, no rights may derive from this white paper. Spotler does not accept any admission of liability for the contents of this white paper. Suggested modifications to the MailPlus software can, as a result of new insights into the GDPR, differ from the actual modifications in the January 2018 release.

Spotler
Boris Pasternaklaan 16
2719 DA Zoetermeer
The Netherlands

(+31) 079 - 363 70 60
contact@nl.spotler.com