Check—
list

CloseAlert

GDPR cheatsheet

Everything you need to know to apply sound data governance policies to CloseAlert.

Customers are willing to share relevant data if that is directly tied to a superior customer experience. Research has found that consumers' trust highly correlates with loyalty and advocacy. However, due to ever increasing data breaches they have become wary of companies asking for information.

As a company you earn trust by demonstrating that shared data is used for a better customer experience. You should further reassure consumers that you take their data privacy seriously by having the governance in place to protect it.

CloseAlert provides a tool to ask for customer feedback through email. It allows the email marketer to understand the feeling and needs of email subscribers and take action to improve.
This cheatsheet will explain all steps to take in order to win your customers' trust and encourage them to share feedback and information.

Inform

To exist harmoniously in the Privacy Paradox, consumers need to pay attention to what they agree to and as a company you need to be transparent. Make sue to inform your audience why and how you collect and use their data!

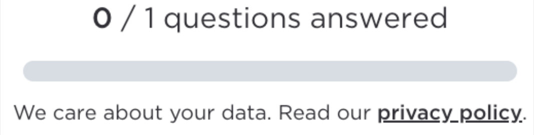
1. Include your privacy policy

This is perhaps one of the most important actions to take.
Include a link to your privacy policy on all your forms, where you explain what is done with the provided data/ feedback.

The EU GDPR contains rules on providing a privacy policy for all respondents. Good practice recommendations include that this policy is:

- concise, transparent, intelligible and easily accessible
- written in clear and plain language

In CloseAlert, you set-up a default link to your general privacy policy. This is a project setting, hence a one-time action. Once done, every CloseAlert form you create within this project includes this link in the footer;



0 / 1 questions answered

We care about your data. Read our **privacy policy**.

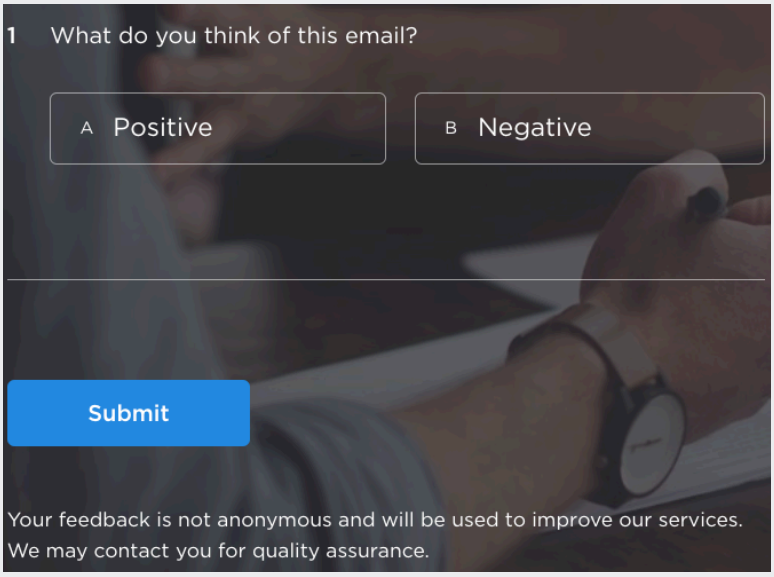
Though we recommend to have the content of your privacy policy checked by your privacy officer, you'll at least have to address the data collection and processing of (email) feedback. A few recommendations;

- You may choose to name the processor (CloseAlert) but it's not mandatory;
- Inform the respondent whether or not data is processed by an external party;
- The data processing purpose will have to be addressed, for example;
    - Data/ feedback collection for the purpose of
        - improving the general client services and communication;
        - addressing questions and/ or solving problems mentioned;
        - improve company processes and communication;
        - sending personal offers based on the feedback.
- Address the legal basis for the data processing (most likely consent).

2. Use the general statement

Make use of the general statement, which can be used to further explain your data security practices. Just as for setting up the privacy policy, the statement may contain a hyperlink.
Advantages of using a general statement in conjunction with your privacy policy;

- Longer text option for elaborate explanation/ information;
- Form specific allowing for use-case specific messaging.



1 What do you think of this email?

Your feedback is not anonymous and will be used to improve our services. We may contact you for quality assurance.

Recommended reading

[Set-up your project wide privacy policy](#).
[Include a form specific privacy policy.](#)
[Include a general statement via your form’s settings.](#)

Data Management

Consumers may be reluctant to share data out of the fear for insufficient protection and possible misuse. As a company you earn consumers' trust by being transparent about measurements you have in place to protect this data.

✓ 1. Anonymize feedback data

Depending on the purpose for feedback/ data collections, it may not be necessary to collect Personal Identifiable Information (PII), such as an e-mail address.

Consider turning off the capturing of an e-mail address through your project settings. Doing so, will guarantee feedback will never include the respondent's email address!

An alternative to anonymized feedback is to captured a hashed ID instead of an e-mail address. This will encrypt the specific information only to be decrypted within your own database again. Though not anonymous, the PII is not legible and more secure.

✓ 2. Have your data retention policy in place

For quality assurance purposes, you may need to capture your respondent's PII and you'll likely want to have that available for a period of time. However, it's unlikely you need to store this PII indefinitely within CloseAlert.

As a best practice, enable the data retention policy. It will ensure that PII data is automatically purged after the time frame determined.

Recommended reading

Anonymize feedback data though your ESP settings.
Include a hashed ID by adding a merge tag.
Have PII periodically deleted by enabling your data retention policy.

Access

Consumers are more likely to do business with your company if they trust you to adhere to GDPR. This is supported by studies proving that, companies with high annual revenue growth are most likely to have superior customer security practices in place.

1. Enable 2 factor authentication

Two Factor Authentication (also known as 2FA or multi factor authentication) is a two step verification method for every log-in. It is an extra layer of security that requires a verification code in addition to your password and username to gain access to the portal.

Enabling 2FA, limits the risks should your password and/ or username ever be compromised. The way it work is, that after you log in with your username and password, you'll receive a verification code per sms. Once you provide the correct code at log-in, you will be able to access the data.

Recommended reading

Enable two factor authentication through your personal settings.

To conclude

The installment of GDPR has raised the bar for data security significantly. The discussions leading up to the enactment of the regulations have increased the public's awareness around data capture and utilization. At the same time, it's caused a fair amount of unrest and uncertainties for the email marketer who's largely dependent on their consumers' insights.

Whilst today's consumer expects personalized communication and tailored experiences, numerous data breaches with services that have taken a prominent place in our everyday lives, have caused the public to mistrust companies requesting too much personal information.

Tight data privacy policies may at first seem daunting and paralyzing for businesses but in fact research reveals a truth in it actually being an opportunity. Consumers put trust in GDPR and if you are able to prove your company takes GDPR seriously, consumers will put trust in you.

Contact details

Want to learn more or have any questions about this step-by-step guide?