SecuMailer

Secure emailing in accordance with GDPR

SecuMailer is the solution for e-mailing personal data in accordance with the GDPR legislation

Website
www.secumailer.com

Whitepaper
GDPR

Content

Introdution

Since 25 May 2018, the General Data Protection Regulation (GDPR) has been in force within the European Union. In the Netherlands, this law is better known under the name “Algemene Verordening Gegevensbescherming” or the AVG. The purpose of the GDPR is to guarantee the privacy of citizens by protecting personal data.

Although the GDPR has been in effect for several years, many organizations are still struggling with it. They are only allowed to share personal information with others under strict conditions and notice that this is at the expense of their productivity and flexibility. That is annoying, because as an organization you naturally want to comply with the GSPR rules and regulations, but at the same time it is also important to communicate quickly and easily with customers, patients or partners, even when it comes to personal data.

SecuMailer for the perfect balance between security and userfriendliness

SecuMailer is the perfect solution: e-mailing with guaranteed encrypted delivery and without cumbersome processes, customer-unfriendly portals or file share servers. With SecuMailer you can send e-mails just like you always did, but in a secure way. The software automatically performs a number of checks in the background to ensure that all e-mail traffic goes through an encrypted connection and complies with the AVG guidelines. As a user you will not notice this. Ideal for both the sender and the recipient.

In front of you is the extensive functional and technical description of the measures that SecuMailer applies to e-mail securely in accordance with the requirements of the GDPR. The document consists of two parts. The first part is intended for readers who want to know more about the functional operation of SecuMailer. In the second part, we focus on IT specialists and go deeper into the technology.

SecuMailer
+31320337381
info@secumailer.com
www.secumailer.com

1. Funcionality

1.1 The basics

To prevent data leaks, it is important to send all e-mail traffic over an encrypted connection. To prevent data leaks, it is important to send all e-mail traffic over an encrypted connection. That seems simpler than it is, because traditional e-mail contains a technical flaw. If the recipient's e-mail server does not support encryption, the message will still be forwarded unencrypted with all the associated risks.

That is why SecuMailer has developed a solution that guarantees the e-mail is delivered over a secure connection. Our e-mail server only forwards the message to the receiving e-mail server if it has confirmed that it supports an encrypted connection. If we are sure that all connections are encrypted (in 98% of all cases), we forward the e-mail so that it directly arrives securely in the recipient's mailbox. If an encrypted delivery is not possible, the recipient is given the option to retrieve the e-mail using an SMS code.

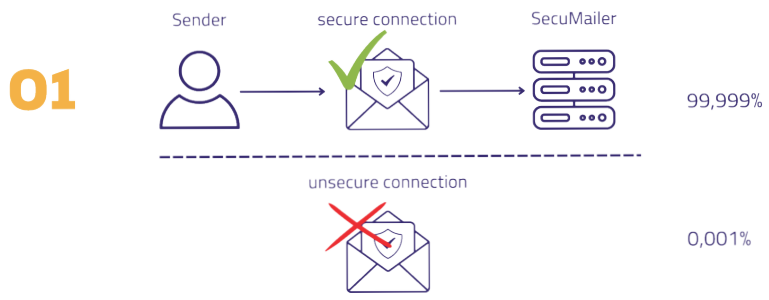
How does it work?

When the user sends an e-mail, we check with both the sender and the recipient whether there is an encrypted connection. We do this using the worldwide TLS standard, also used by banks, governments and security organizations.

The process consists of 3 steps:

Step 1: Check the sender

First, we check whether the sender communicates with us via an encrypted (TLS) connection. In principle, this is always the case because we check by default whether a new SecuMailer customer has implemented TLS.

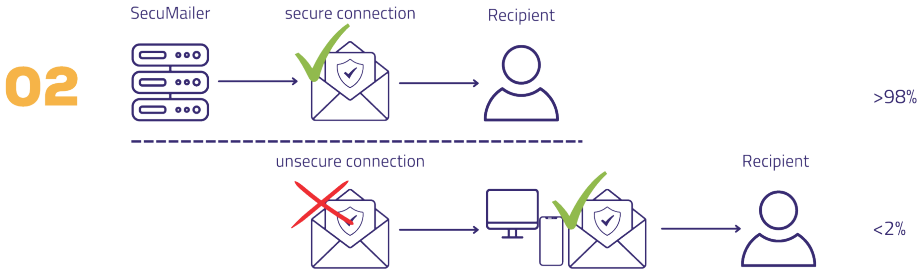


Yet we always check the connection, it may happen that something goes wrong over time because, for example, a certificate has expired. If a sender wants to send an e-mail via SecuMailer without valid keys, it will not arrive at our server. That is why we continuously monitor e-mail traffic. If we see that the e-mail traffic is at a standstill, we immediately inform the customer and help him to get the e-mail traffic going again. Fortunately, in practice, this rarely or never happens.

SecuMailer
+31320337381
info@secumailer.com
www.secumailer.com

Step 2: Check the recipient

The next step is to check whether we can set up an encrypted connection with the recipient. This works in 98% of the cases!



Sometimes we fail to set up an encrypted connection and then we will choose an alternative route. We temporarily store the message in a well-protected environment and send the recipient by e-mail a request to retrieve the message using a code that we send via SMS. Of course we do need the recipient's phone number for this. If we do not have this, we will send the sender an e-mail with the request to enter the number., That's how SecuMailer guides users through the process very simply.

Step 3: Digital Signature and Delivery

Once we are sure that the message is going over an encrypted connection, we digitally sign the e-mail and forward it to the recipient. SecuMailer automatically sends a digital signature with all outgoing e-mails. This guarantees the integrity of the e-mail and prevents unnoticed changes to the e-mail.

SecuMailer records all information about the transmission and delivery in real-time in a log file that is accessible via the administrator portal. This log forms the indisputable proof of delivery (as with a digital registered letter).

Impact of SecuMailer on your organization

All this has no impact on the local environment of the users. We link SecuMailer to the customer's e-mail server. This has the following advantages:

- No adjustments are necessary in the e-mail environment of the users.
- SecuMailer guarantees an encrypted connection for all e-mail traffic. Employees do not have to do anything extra for this. They e-mail like they always do.
- Recipients simply receive the e-mail in their inboxes.
- Minimal management.

SecuMailer
+31320337381
info@secumailer.com
www.secumailer.com

1.2 Extra functionality

In addition to sending e-mails securely, SecuMailer offers a number of additional services:

1. Sending large files

SecuMailer users can send up to 40 MB of attachments by e-mail by default. In addition, we offer an Outlook plug-in (2013 and higher) that makes it possible to securely share large files of up to **5 Terabytes**!

All files are securely stored within the EEA. The customer determines how long they are kept (maximum 90 days). After that, they are automatically destroyed.

How does the SecuMailer Outlook plug-in work?
After installing the Outlook plug-in, you as a user will see an extra menu option in your e- mail program. This allows you to upload large files to a secure environment. After uploading, SecuMailer automatically adds a link to the e-mail. The user sends that e-mail incl. link via an encrypted connection to the right person. Via this link, the recipient of the e-mail can download the file with one click.

From Q2 of 2022, we will introduce a new version of the plugin. You can also make these available to customers to securely exchange large files or collaborate on documents.

2. Securely send automated mail

We have developed an API link to integrate SecuMailer with the back office and securely send automatically generated e-mails. Such a link is particularly interesting for organizations with applications that generate large flows of personalized e-mails and who want to be sure that all those messages arrive securely in the recipient's mailbox via an encrypted connection.

2. Technology

SecuMailer
+31320337381
info@secumailer.com
www.secumailer.com

SecuMailer is an innovative platform based on the most modern cloud technology from Amazon, serverless computing and event based computing. We meet the most stringent requirements in the field of e-mail security and are ISO 27001/:2017, NEN 7510: 2017 and NTA 7516:2019 certified.

Unlimited scalability

SecuMailer's software is fully cloud-based and runs as SaaS from Amazon in the EU. If necessary, we can scale from a few e-mails to millions of e-mails within milliseconds without any changes to infrastructure or software. That makes us very flexible. In terms of performance or stability, it makes no difference how many users use the application or how intensively they do it. We do not have to make agreements about this with our customers in advance. They e-mail as much as necessary, and only pay for the capacity they actually use.

Serverless Computing

For each (incoming or outgoing) e-mail, we start up its own container (virtual server) that is only accessible by SecuMailer and only for the duration of the processing. As soon as the e-mail has been processed, the container, including the data, will be destroyed again. In this way, no digital trace is left behind and that is very secure! What is not there cannot be intercepted. In terms of data security, SecuMailer is the absolute frontrunner in the market.

E-mail security is our core competence

SecuMailer works with a closed network. This means that we only process e-mails from registered and verified accounts. We check all e-mails for viruses and spam. We do this by using the following standards, among others: TLS, PGP/MIME, SPF, DKIM, DMARC, DANE, MTA STS, TLSRPT, SAML2, OpenID Connect and OAuth2.

STARTTLS and DANE
Starttles ensures a secure connection between sending and receiving mail server DANE enforces STARTTLS and provides assurance about the identity of the receiving mail server. DNSSEC guarantees the authenticity of DANE in this chain.

SPF
SPF prevents someone from sending an email on behalf of your organization. SPF checks the sender of an email for authenticity.

DKIM
DKIM prevents e-mails counterfeiting. If someone tampers with the content of an e-mail, DKIM detects it.

DMARC
DMARC tells your e-mail server what to do if it receives a fake e-mail. DMARC also ensures that an organization receives information about forged e-mails sent in its name.

Public Key Infrastructure

Before we deliver an e-mail, we check whether the sending and receiving parties are using a secure connection. We also check that the secured connection is based on cryptographic key material from a trusted root certification authority.If that is not the case, we offer an alternative way to securely deliver the message to the right person by means of an SMS code.

SecuMailer
+31320337381
info@secumailer.com
www.secumailer.com

3. Security and quality

SecuMailer is a Dutch company. We develop all our software with user security and privacy in mind. We use cloud computing services from AWS Dublin and Frankfurt. AWS has direct agreements with the European Union about privacy laws and the measures needed to ensure that no data from European companies falls into American hands.

Data minimization

The messages you send via SecuMailer are 100% secure with us. We can't see them, and we don't store them. An important principle in the GDPR is data minimization and we strictly adhere to it: we do not process data that we do not need, so that we do not run unnecessary risks.

Very concretely: we immediately forward the e-mails that we transport. We do not do anything with them and do not store them. We only log the transport data (metadata about the e-mails). This logging is necessary to prove that the message was actually delivered encrypted.

Only if we do not forward the message immediately, because the recipient does not have a secured connection, we store the encrypted (unreadable) message for a maximum of 90 days. We do this in a secure place in the cloud and once the message has been retrieved or the retention period has expired, it is also deleted again. So you don't have to worry about major data leaks at SecuMailer. We are Secure by Design!

Transparency and equality

The GDPR states that employers must take measures to prevent human errors.
That does not mean that you can just monitor the e-mail behavior of employees to, for example, check whether they are ignoring certain warnings. It is better not to give the user a choice, and to include business rules for this in the software.

The right to privacy and transparency also applies to those who receive the e-mail. It is at odds with the GDPR to monitor when or where a recipient reads their mail. At SecuMailer we solve this in a different way. We record exactly in the logging when the message was sent encrypted to the recipient's mailbox .With this confirmation of delivery, you fully comply with your information obligation from a legal point of view.

Actively facilitating the BCC field is also at odds with the transparency principle of the GDPR. Communication by e-mail must always be transparent and equal.

Our choice for data minimization and transparency has a number of functional consequences. For example, SecuMailer deliberately does not support the following functions:

- Withdrawing sent messages
- Monitoring employee e-mail behavior
- Read receipt recipient
- Send e-mail with BCC

SecuMailer
+31320337381
info@secumailer.com
www.secumailer.com

Safety first

SecuMailer guarantees customers that all their message traffic goes through an encrypted connection and is therefore GDPR compliant. We have hard evidence of that. We had an IT security assessment performed by Securify, which determined that SecuMailer meets all security guidelines and is of high quality.

External audit confirms it: SecuMailer is 100% GDPR-proof!

Some quotes from Securify's report:

"SecuMailer provides a secure e-mail platform to customers. All e-mail communication is performed over GDPR-compliant secure channels. If a remote server does not support a secure (TLS) connection, the e-mail is blocked to ensure that no information is transmitted in clear text."

"Securify has performed several tests but has been unable to compromise the SecuMailer platform during the assessment. SecuMailer is being built with security in mind, giving the platform a secure foundation for future development."

"The overall security level of SecuMailer is good. The developers clearly use a defensive style with security in mind as they are developing the program. This ensures that the end product will be more secure from outside attacks."

"Securify was not able to find any way for an outside organization to obtain data and / or e-mails from other organizations."

SecuMailer
+31320337381
info@secumailer.com
www.secumailer.com

4. Implementation and Management

4.1 The implementation

SecuMailer connects with a mail relay on the e-mail server and therefore has no influence on the client environment. The technical implementation is very simple. The customer needs about half an hour to go through all the steps. SecuMailer provides the technical instructions for this and, if necessary, also offers further support.

A plug-in for Outlook 2013 and higher is available to send large files. The administrator manages the installation centrally or leaves it up to the users.

SecuMailer has standard integrations for Office 365, Exchange, Gmail for Business, all common Unix mail servers and Salesforce. We offer a REST API and SMTP API to integrate SecuMailer with back office applications for organizations that want to automate their e-mail flows while guaranteeing secure transmission and reception. The APIs work with open standards and interfaces, making them easy to integrate. There is an extensive description of the interfaces with which customers in principle do this themselves. They receive a special code to connect to the SecuMailer server. If necessary, we can support you with this.

SecuMailer is suitable for all e-mail applications and all devices. When the user sends an e-mail, we check with both the sender and the recipient whether there is an encrypted connection. We do this using the worldwide TLS standard that is also used by banks, governments and security organizations.

4.2 Management

Local SecuMailer administrators have access to their own management portal containing the following functionality:

Events: This concerns the comprehensive audit log in which all information about the shipment and delivery is recorded. This gives administrators insight into all e-mail traffic. If an e-mail is refused (eg with an unknown address), this can also be found in the log. For example, the organization has indisputable proof of all e-mails that have been sent securely, including timestamps, IP address sender and replacement, proof of digital signature, etc.

Accounts: A list of e-mail addresses and telephone numbers that SecuMailer uses to send the recipient an SMS with a code to retrieve the e-mail in the event of an unsecured connection.

Mailbox Settings: The administrator configures a number of settings for each mail domain (eg location and storage period of large files, error messages).

SecuMailer
+31320337381
info@secumailer.com
www.secumailer.com

Experience SecuMailer?

Discover the convenience of SecuMailer and request a free trial account. This allows you to send a maximum of 20 secure e-mails within two weeks. Of course we are also happy to come by for a demo, without obligation, physically or virtually.

Do you have any further questions? Or would you like to receive a non-binding offer? Please contact us via info@secumailer.com or call 0320-337381.

Yvonne Hoogendoorn, CEO SecuMailer