SecuMailer

Whitepaper

Send Email Securely

Why choose email security that gets in your way?

With SecuMailer, you reach your recipients safely and effortlessly.

TÜVNORD TÜV NORD Nederland B.V. NEN 7510 tuv.nl

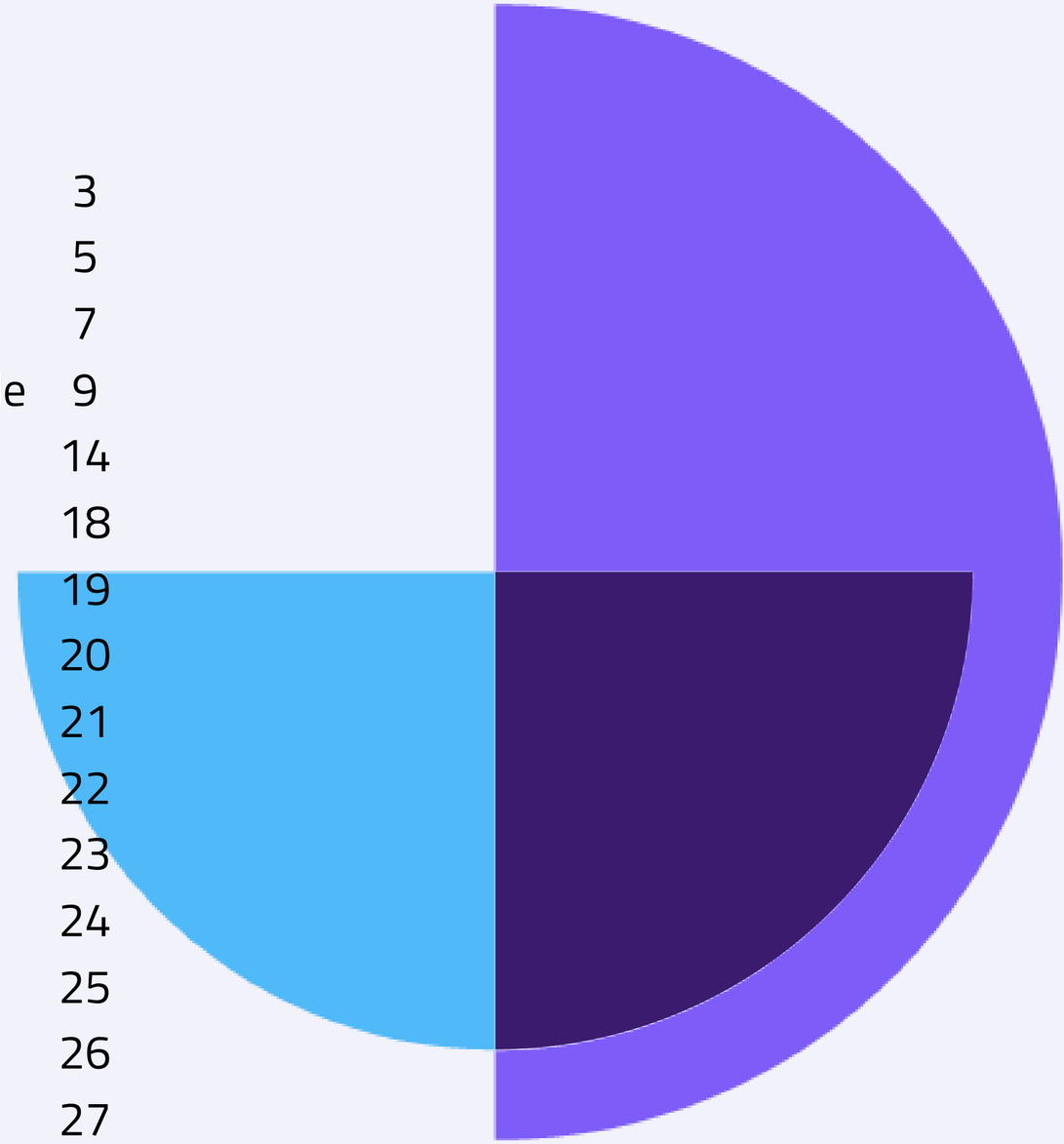
TÜVNORD TÜV NORD Nederland B.V. ISO 27001 tuv.nl

CYBERSECURITY™ MADE IN EUROPE

eIDAS

THIRD PARTY ASSURANCE REPORT ISAE 3000 SERVICE ORGANIZATIONS SOC 2 TYPE II AUDIT COMPLETED

Table of contents



With SecuMailer, you send email securely with the ease of regular email.

What Makes SecuMailer Unique:

- We deliver the contents of your email securely to the recipient’s inbox.
- No plug-ins required—just a direct connection at the mail server level.
- Employees send emails, SecuMailer secures them, and your organization stays in control.
- Never unintentionally insecure again: every email is sent safely.
- Effortlessly comply with all laws and regulations: GDPR, NTA 7516, eIDAS, NIS2, and DORA.
- Complete data sovereignty: your data stays within Europe.

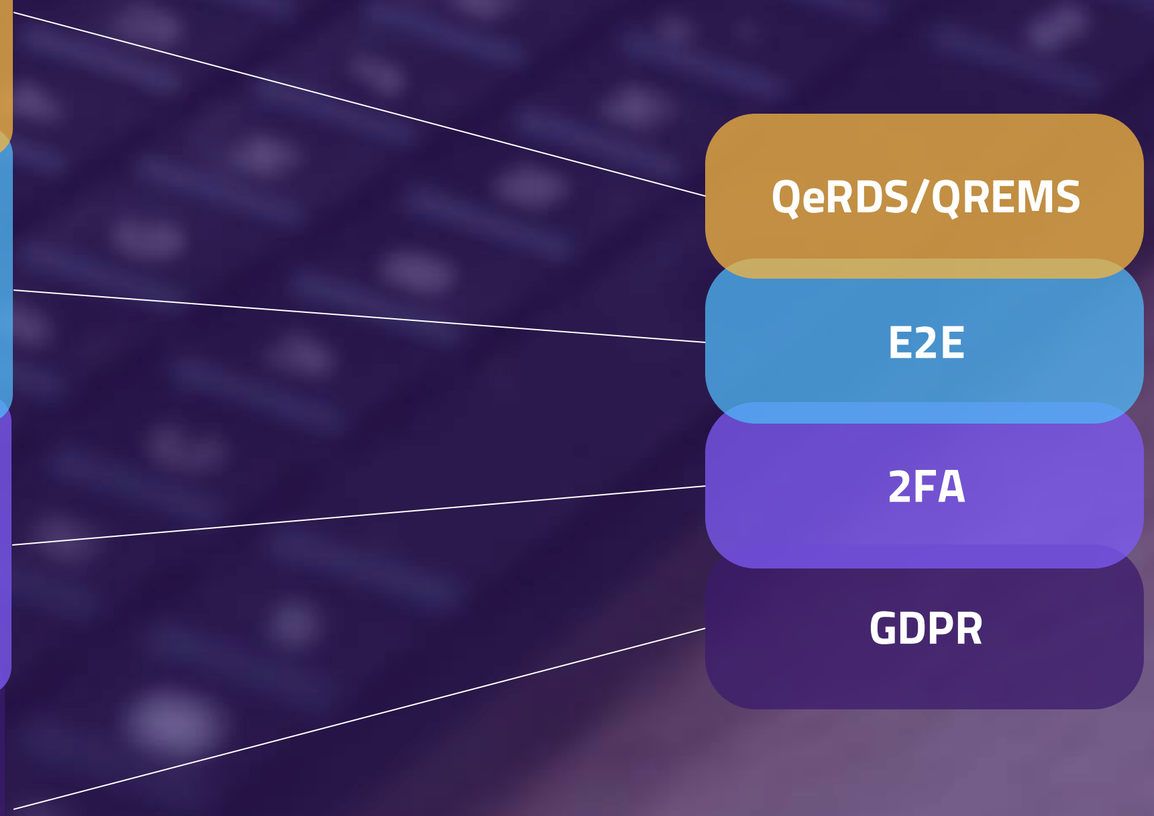
SecuMailer’s 4 security levels

At the highest level, QeRDS/QREMS, which exceeds both the medium and high levels with additional proof of delivery.

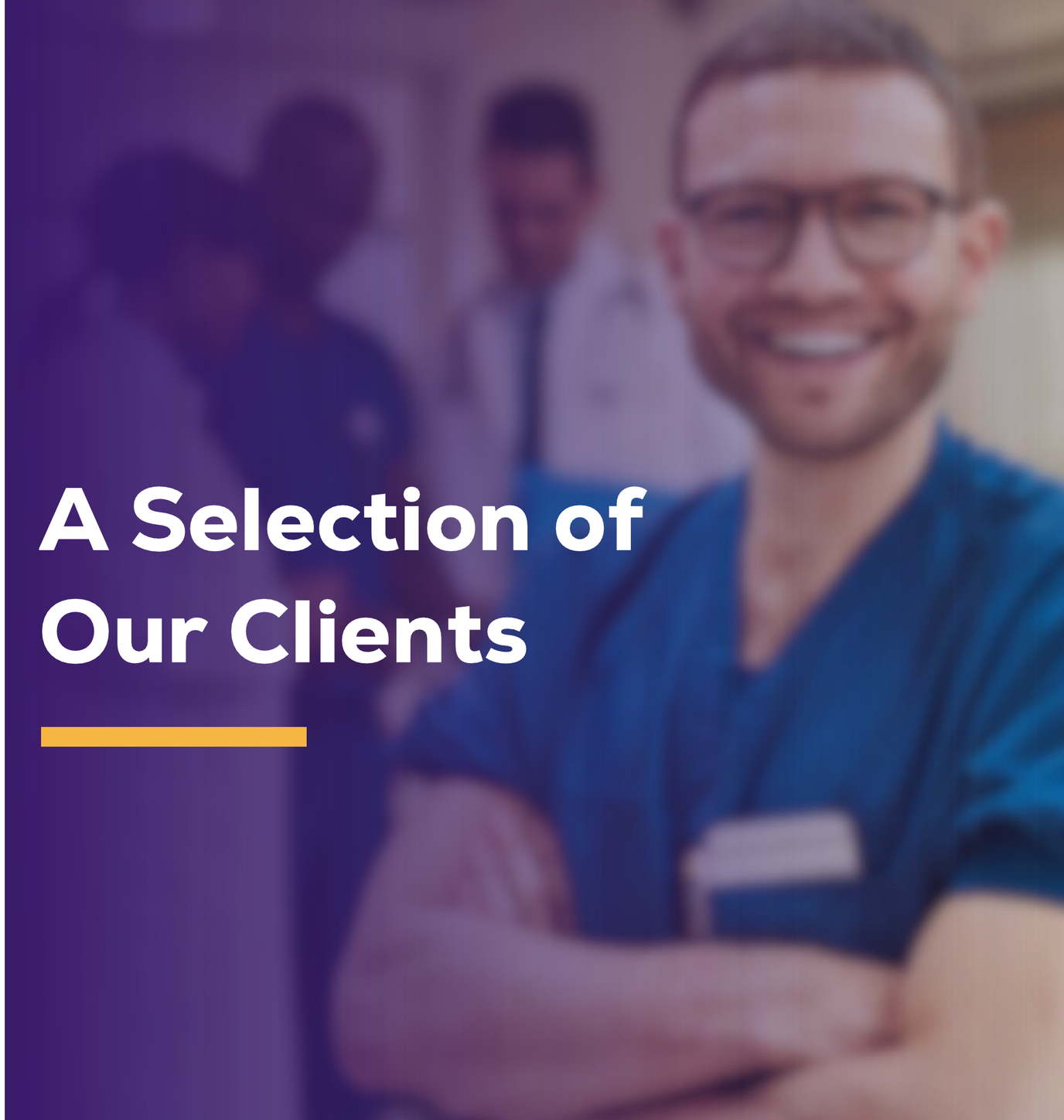
At a high level, E2E for highly confidential data using end-to-end encryption.

At the intermediate level, 2FA secures confidential data by applying two-factor authentication for the recipient.

At the basic level, GDPR for non-confidential personal data.



A Selection of Our Clients



Why SecuMailer?

Proven Compliance and Legally Binding Email Communication

GDPR

- Secure transport: TLS 1.3, DANE, DNSSEC
- No content storage, data remains within the EU
- Independent security audit: “SecuMailer is 100% GDPR-compliant.” – Securify

eIDAS Qualified Registered Electronic Mail Service (QREMS)

- Legal proof of identity, integrity, and delivery
- Recognizes electronic delivery as legally valid (‘digital registered mail’)

BSI TR-03108-1 Secure E-Mail Transport

- SPF, DKIM, DMARC, logging, 2FA, TLS protection
- Automatic fallback to encrypted portal for insecure mail servers

ISO 27001 / NEN 7510 / NTA 7516

- For medical, legal, and government communication
- Full audit trail and proof of receipt

How can you send confidential information securely without sacrificing time, convenience, or focus on your work?

It’s essential to protect confidential data.

On paper, this sounds good, but in practice, it often means:

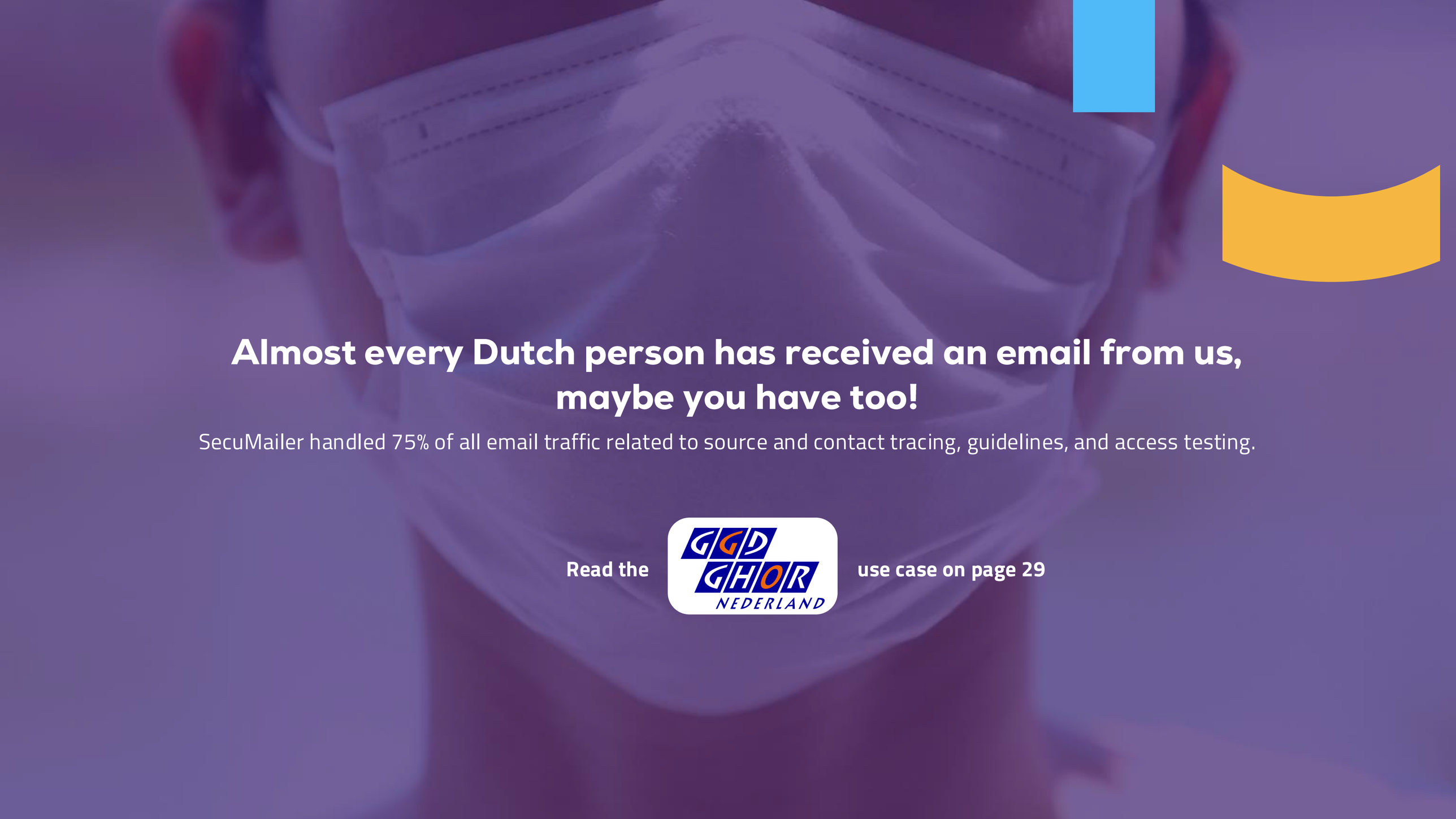
- Frustration from dealing with codes
- Time-consuming tasks that distract you from your work
- Recipients not opening emails because there are too many steps

Ideally, people want to send a regular email, but that’s not secure. SecuMailer makes it possible! By managing the security level centrally, employees no longer have to think about email security. No extra steps, no plug-ins, just email.

The result? More time for core tasks, less frustration, and 100% compliance with every email.

Share Confidential Data: Easily Comply with GDPR and NIS2

- For personal and confidential data
- 2FA via SMS code
- Authentication remains valid for up to 90 days instead of logging into a portal for every message
- Maximum of 4 SMS messages per year
- Interoperability as part of the secure email providers’ interoperability network
- Emails are always where you expect them: in your inbox and the recipient’s inbox



Almost every Dutch person has received an email from us, maybe you have too!

SecuMailer handled 75% of all email traffic related to source and contact tracing, guidelines, and access testing.

Read the GGD GHOR NEDERLAND use case on page 29

How SecuMailer Makes Secure Emailing Both Safe and User-Friendly—Without Compromise:

Preserve the Email Experience

After your recipient has authenticated, we deliver the email directly to their inbox. Once delivered, the data is removed from our server, just like a mail carrier with an empty bag after dropping a letter in the mailbox. Your organization stays in control: you decide how long authentication remains valid (up to 90 days). In the meantime, we securely deliver all emails to recipients, fully compliant with GDPR, NIS2, eIDAS, ISO 27001, BIO, and NTA 7516.

Always Compliant: GDPR, ISO 27001, NTA 7516, eIDAS, NIS2, and DORA

By implementing SecuMailer, your organization will always be 100% compliant with all applicable laws and regulations for secure email communication. Our privacy experts are fully up to date on every detail. Together with our product, they help you meet all requirements in the areas of privacy and security.

No Plug-Ins Required

SecuMailer works in the background without requiring you to install extra software. No hassle with updates or compatibility issues, just simple and effective! Thanks to a mail server-level integration and our AI-driven DLP, IT management overhead is virtually zero.
Want active user support directly in Outlook? That’s possible too. Use our web-based Add-in, which doesn’t interfere with the client, always includes the latest security updates automatically, and works seamlessly with Windows updates.

Security Level Centrally Managed

By moving the security level from the employee to a central point within the organization, employees no longer need to think about secure emailing. This allows them to spend the time they save on their work without risking insecure emails. As an organization, you decide who emails at which security level and what exceptions apply. You can easily configure this via the management portal. Our DLP solution can also be used for this.

EU Data Sovereignty

Our servers operate exclusively within the European Cloud. Through Data Haven, our customers can store emails in their own private cloud environment. SecuMailer does not retain unnecessary data. As soon as the email can be delivered (after recipient authentication), it is retrieved from the customer’s Data Haven and delivered. This guarantees data minimization.

Cloud Sovereignty in NL

Starting in Q1 2026, SecuMailer will be available in a private cloud in the Netherlands. From then on, our customers can choose to have the SaaS platform hosted in a Dutch private cloud environment. This makes full independence from AWS Europe possible. The influence of foreign legislation, such as the Cloud Act, and potential “blackouts” due to U.S. policies will be completely eliminated. As a result, all risks to business continuity are mitigated.

Raad voor de Kinderbescherming
Ministerie van Justitie en Veiligheid

The Child Protection Board has been a client since 2022.

“On average, we send 130 business emails per day. But this also needs to be done securely.”

Read the complete case ››

The challenge

Maintaining privacy and complying with regulations for secure emailing are essential, as a large amount of personal data is exchanged via email.

Ease of use for end users must be optimal. There is frequent communication with individuals such as parents, foster parents, and guardians.

Technical integration should be simple and align with existing cloud-based workplaces.

The solution

In September 2022, the Child Protection Board implemented secure emailing with SecuMailer.

The result

By maintaining the familiar email experience, we deliver an **excellent user experience** without reported issues.

Fully compliant with laws and regulations.

Secure emailing **integrates seamlessly with cloud-based workplaces** without the need for a plug-in.

One solution, loved by all involved

Users

No more worries or hassle with Secure Email. Users simply send emails from their trusted email client, without any extra steps.

Admins / IT

SecuMailer integrates seamlessly into your existing work environment. The mail server is connected to the SaaS platform via a mail relay. Required maintenance is minimal. Delivery receipts, reports, and REST API integrations are available. The solution is so simple that anyone who can send an email can use it immediately, without training and without support.

Privacy & security officers

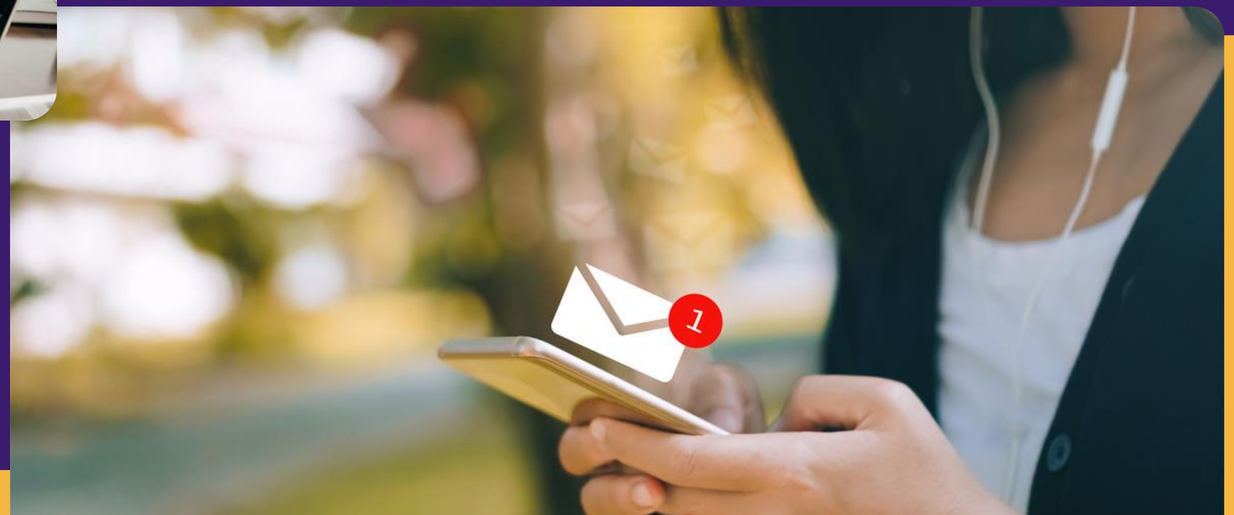
SecuMailer complies with all relevant standards, including ISO 27001, NEN 7510, eIDAS, NTA 7516, ISAE 3000, SOC 2 Type II, and the ECSO label. Just like a mail carrier who delivers a letter and then has nothing left in the bag, SecuMailer securely delivers the email without unnecessarily storing any data.

Management team & Procurement

You only pay for what you use and save on maintenance thanks to low IT overhead. At the same time, you minimize the risk of fines or reputational damage because the product is always on. Thanks to continuous innovation, you’re ready for the future.

Recipients

The email simply arrives in the inbox, exactly where the recipient expects it. Authentication is only required once every 90 days (by default). In the meantime, the recipient enjoys a normal email experience with the healthcare provider.



SecuMailer

1. Cloud Sovereignty
   Fully Dutch company, ECSO Label, private Dutch cloud
2. Data minimalization
   Emails are not stored: What isn't stored can't leak.
3. No plug-in
   All functionalities work through the standard email application.
4. Centrally Managed Security Policy
   Every email is always encrypted, never accidentally sent insecurely.
5. Email from any device and mailclient
   a.o. Outlook and Google Workspace, from laptop, phone and tablet
6. Just email, no training required
   Secure Email doesn't have to be complicated
7. Data Haven
   Your email in your own cloud

VS

Alternative solutions

1. USA influence/ dependency in company
   Highly vulnerable to foreign legislation such as the Cloud Act
2. Data concentration
   All emails are stored in one place, posing a significant risk
3. Plug-in needed
   Use of plug-in has impact on IT, workplace, and sender
4. Choice for security lies with sender
   Greater chance of human error.
5. Only Outlook is supported
   Because of dependency on plug-in
6. Extra steps for sender
   Different method of sending (not the same as regular email)
7. No data sovereignty
   Third copy of confidential emails with supplier


Functionalities

Functionalities SecuMailer

What functionalities are available?

- **Standard encryption:** All emails are sent encrypted by default
- **Digital signature:** SecuMailer adds a digital signature to every email
- **Proof of delivery:** SecuMailer records who sent and received a message, and when
- **Authentication:** Option to enforce 2FA for specific emails or users
- **DLP and business rules:** Ability to set rules for automatically applying security based on email content
- **API integrations:** Connections with various systems such as CRM, EHR, and ERP

Functionalities for admins

Admin portal:

- Log email traffic data
- Register phone numbers and other 2FA options
- Organization-specific settings for domains, exceptions, and DLP
- Reporting capabilities
- Access to online manuals, technical documentation, and a support team
- Sender and recipient portals are also available, allowing users to modify and manage certain chosen settings themselves

Large files | SecuFiler

With SecuFiler, you can securely share large files—up to 5TB—via the Outlook add-in or the SecuFiler web application.

- **Sharing via browser:** Integrate SecuFiler as a page on your organization's website. Through this page, your employees and customers can easily send all confidential documents securely to and from your organization.
- **Wide range of file types** such as .pdf, .jpg, .png, and .mp4
- **Suitable for medical information:** With the option to apply 2FA, you can securely send large files in compliance with NTA 7516 requirements.

Registered Email

Send a registered email with the same legal status as a registered letter. SecuMailer is eIDAS certified for this purpose.

- SecuMailer is fully certified for eIDAS Qualified Registered E-mail Service QREMS and is on the EU trusted list.
- There are two possible applications:
- **Qualified registered email:** a qualified email has legal status and can be used as legally valid evidence
- **Sent by registered mail:** possibility to request a proof of delivery for sent emails, verifiable that the content of the email has not been altered, and that the recipient has been identified. The legal status is valid within the Netherlands, but is not sufficient in a European context

BVCM is a client since 2022

“We spoke with three companies that offered a similar solution, but SecuMailer stood out head and shoulders above the rest.”

[Read the complete use case ››]

The challenge

BVCM sends sensitive information to clients, debtors, and courts daily. When legislation changed, secure email became a necessity. For them, one thing was clear: it had to remain practical for employees, without extra hassle or unnecessary tools.

Clients expect agreements to be honored and communication with debtors to actually take place. This required a solution that not only guarantees security but also provides insight into any delivery issues.

The solution

In 2024, BVCM integrated QREMS registered email with their debt collection backend system.

The result

With SecuMailer, BVCM saves time, money, and worry. Emails are demonstrably secure and legally valid, without hassle for employees or recipients. Sending registered emails is now efficient through eIDAS mail. Employees can focus on their work while email security runs seamlessly in the background.

Corporate functions:

- **REST API connections:** connections to various back-office systems
- **Mail merge:** option to send personalized bulk emails
- **SAML:** Single sign-on (SSO) functionality for access to the management portal
- **SIEM/SOC RBAC:** possibility of integration with Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) systems
- **Custom branding:** customization of the branding of notification messages and the web interface
- **Data Haven:** Temporary storage of secure emails awaiting delivery, at a location of the organization's choice
- **Private Dutch Cloud:** Complete handling of secure email processing within the private cloud in the Netherlands. This ensures complete exclusion from influence of foreign legislation such as the Cloud Act and "being blacklisted"

End-to-end

- **Always encrypted:** The content is fully encrypted from sending to receiving, even in the recipient's mailbox
- **Authentication** possible via DigiD, SMS, or other ID methods
- **Full control over the information by the sender:** The message is always encrypted, both during transport and in the recipient's mailbox. If the sender revokes the key, the message can no longer be read, even after delivery to the mailbox
- **Suitable for your own DLP**: Sender sends secure email via encrypted connection to the SecuMailer platform, where e2ee is applied. This gives the sending organization complete control and insight into what information the organization (may) leave
- **Advanced browser decryption:** Full decryption takes place locally, in the browser's memory. This means that no collection of certificates is required from the recipient, making this method of e2ee highly suitable for residents and patients
- **Certification:** Full compliance with ISO 27001, eIDAS QeRDS/QREMS, NTA 7516, and GDPR

How end-to-end encryption works

When a message is sent via SecuMailer, it is first transmitted over a secure connection and then end-to-end encrypted before reaching the recipient’s mailbox. The message remains encrypted in the mailbox, not on an external portal.

The recipient doesn’t need to install or configure anything. Using a secure link, they open the message, and decryption takes place locally in the browser. The required keys are generated temporarily in the browser and never leave the recipient’s environment.

This means:

- The sender sends securely, without certificate management.
- The recipient reads securely, without extra software.
- No one, not even SecuMailer, has access to the content.

Experience the convenience of regular email with the security of end-to-end encryption, without the complexity of S/MIME.

GGD-GHOR is a client since 2021

Up to 1 million emails securely sent per day during the COVID-19 pandemic.

[Read the complete use case ››]

The challenge

- Need to be able to scale up quickly to send up to 1 million emails securely per day
- Ease of use for users must be optimal. Emails are mainly sent to citizens
- Medical data must be able to be emailed while complying with European laws and regulations

The solution

Since 2021, GGD GHOR has been using SecuMailer's mail merge solution to send more than 50 million emails containing medical information to citizens.

The result

- No data breaches
- No security incidents
- No impact on the service desk

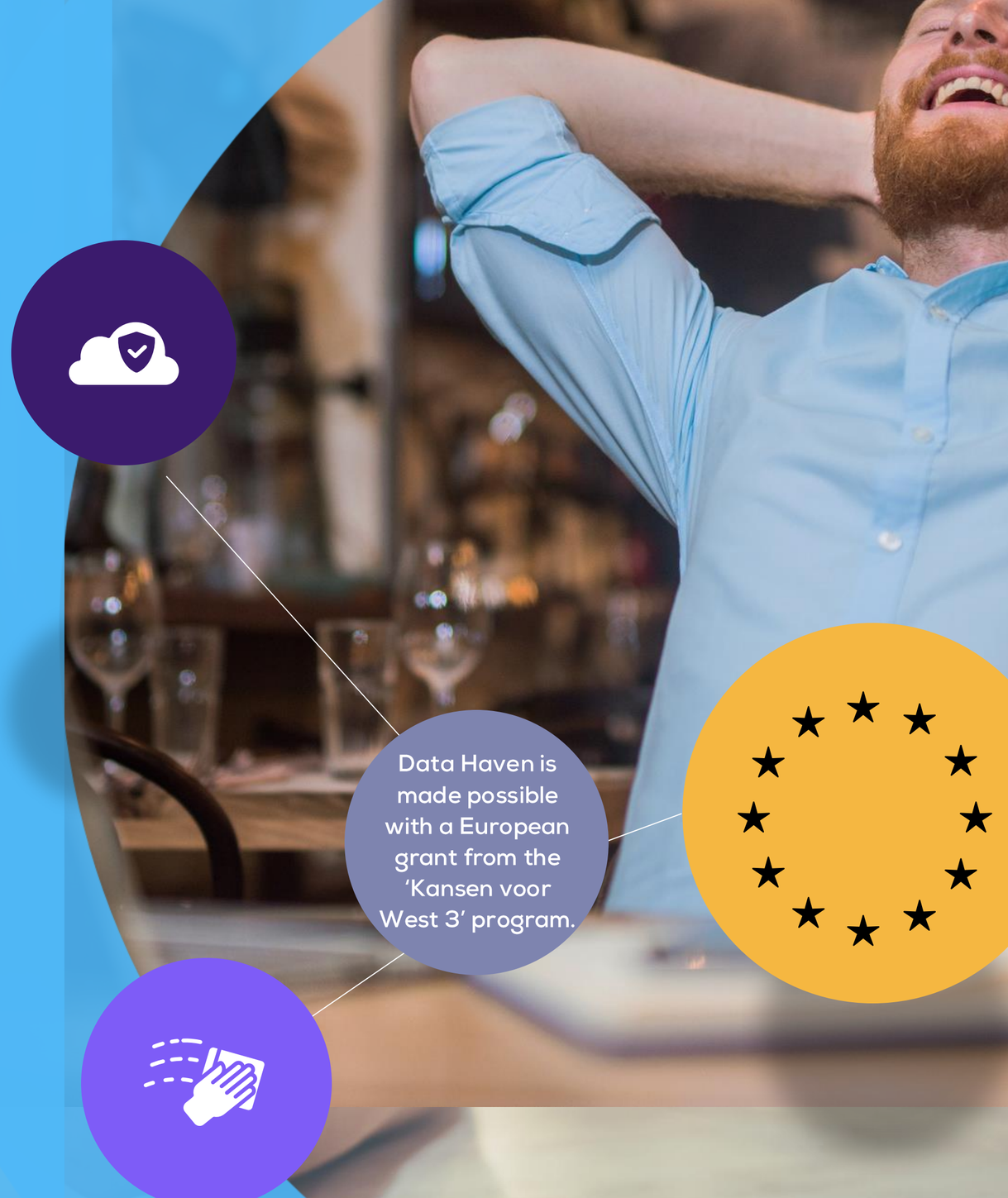
Gefinancierd door de Europese Unie

Data Haven

Complete data sovereignty: Enables your organization to store emails temporarily (this is necessary if the recipient still needs to authenticate) within its own (cloud) environment instead of on external servers.

100% European solution: Data Haven offers your organization the assurance that your data for Secure Mail is fully subject to European supervision and hosted within the EEA, supported by the ECSO quality mark and developed with the help of the ERDF program.

Data minimization as a starting point: Messages and attachments are deleted immediately after delivery. The email message that is temporarily stored before delivery is kept secure in the customer's own environment with Data Haven.



Data Haven is made possible with a European grant from the 'Kansen voor West 3' program.

Want experience SecuMailer yourself? Plan a demo!

Contact us:

www.secumailer.com

info@secumailer.com

+31 320 337 381

Or schedule your meeting directly:

Schedule a demo (no strings attached)