

# StealthMail helps you with GDPR compliance, makes your emails secure & invisible

Avoid severe GDPR penalties & legal risks, don't lose your reputation, emails and digital infrastructure



91% of attacks and data breaches start with email because it's based on the outdated 1982 protocol, while the new GDPR rules set severe penalties up to €20M or 4% of global annual revenues.

StealthMail makes your emails secure and invisible to email relays, hackers or Public Internet threats, making email relationship with clients a trusted one via best-in-class StealthMail's Secure Email Channel.



## Why customers use our service?

- GDPR sets new requirements for Security of processing, and Data protection by design and by default
- SMTP (or Email) sends personal data over Public Internet in clear text, without encryption
- StealthMail never sends personal data over Public Internet
- The integration is seamless with Outlook and Azure

## Email GDPR compliance

- Article 25. Data protection by design and by default
- Article 32. Security of processing
- Article 33. Notification of a personal data breach to the supervisory authority

## Military Grade Cyber Security

- Email (SMTP) is used to send crypto-URLs only;
- Emails and files never leave your secure perimeter & are stored in your protected cloud;
- Control over keys, crypto machines and data

## Seamless Integration

- Users install Outlook Plug-In
- StealthMail is deployed to your Azure account

**Emails and data sent via StealthMail will not be exposed to open mail relays or Public Internet**

**When user loses login and password, email data is not exposed, just the crypto-URL**

**Outlook Plug-In / Azure**

StealthMail helped us solve our major data privacy & compliance risk – human factor & email communication.

– Nikolay Sakharov, Senior Partner, Sakharov&Partners

# StealthMail deployed on Microsoft Azure + Outlook Plug-in helps clients to minimize GDPR compliance risks, protect email and files



## SMTP 1982 vs. GDPR 2018

- Email internet standard or SMTP (Simple Mail Transfer Protocol) is an unsecure clear text protocol developed in 1982;
- 91% of attacks begin with email, 90% of data leakages can be traced back to user behavior;
- StealthMail Client increases Email GDPR compliance and upgrades cyber security.



## Client-Owned Trusted Cloud

- StealthMail is deployed on client's Microsoft Azure account;
- Client has the full exclusive control over his/her encryption keys, data and access;
- Client creates his/her own segregated secure infrastructure within secured Microsoft Azure.

## StealthMail Offer

### Our promise to you

We will secure your email communication, minimize your SMTP risks and help optimize for GDPR compliance.

### An offer to get you started

- Exclusive and time-limited opportunity to sign up for \$15 per user per month;
- Minimum is decreased to 100 seats from the standard minimum of 500 seats.

## Tangible Benefits / Desired Outcomes

- You will significantly reduce violation risks of GDPR Articles 1, 25, 32, 33 and other;
- Your emails and personal data will not be exposed to open mail relays or Public Internet;
- You will be able to revoke historically sent emails and personal data;
- User device protection;
- Access rights management;
- Panel for Data Privacy Officers and Security Officers.

## Why StealthMail?

StealthMail makes your emails secure and invisible for open mail relays, hackers or Public Internet, and gives you a full exclusive control over your encryption keys, data and access. It encrypts user's emails and attached files individually, so that your content never leaves your secure perimeter.

It's a military grade multilayered business security solution that includes encryption, user rights management, restrictions to access secured data, control over execution of selected operations according to company's security policies with an unparalleled ability to revoke any historical email.