

# Secure Email



Preventing data leaks due to human error in digital communications has never been so easy.

ZIVVER works by monitoring email recipient addresses, messages, and attachment content.

ZIVVER is a secure email platform that focuses on preventing data leaks caused by human error. It protects businesses against the repercussions of data leaks such as reputational damage and GDPR fines. It also protects your customers against unwanted access to their private information.

ZIVVER's Secure Email feature is the most comprehensive and future-proof solution on the market. It works by monitoring email recipient addresses, messages, and attachment content. In case of a threat, ZIVVER alerts the user with a warning that must be addressed before moving forward with sending the email. Even if a mistake after the alert occurs, the platform provides the option of email retraction for original and forwarded recipients. Additionally it is possible to set a message expiration date, this feature is quite useful not only for information security but for other business applications as well.

## Benefits of implementing ZIVVER in your organization



Real-time monitoring of recipients, email, and attachments



Email retraction



2FA for accessing emails



Asymmetrical encryption



Guest user support



Outlook plug-in



Web and mobile applications



Corporate Guest Branding



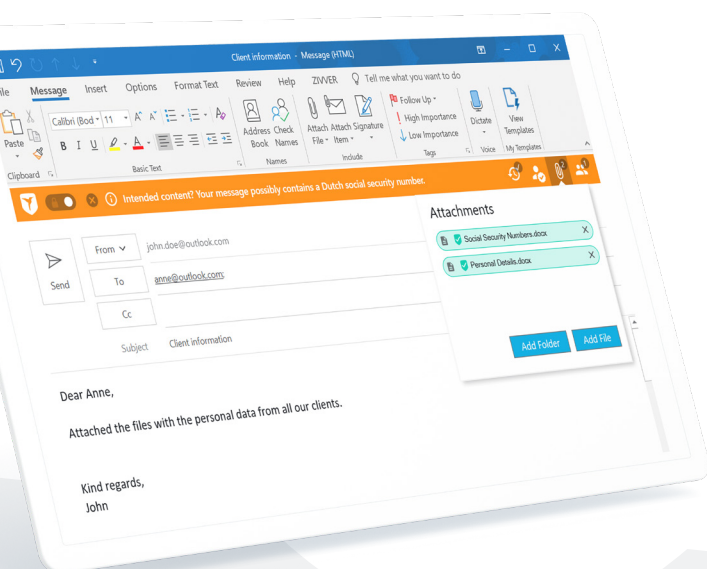
Secure Conversation Starters

## 1 Real Time Classification

ZIVVER's smart alerts help users avoid embarrassing and costly mistakes when sending sensitive information via email. These alerts point to potential risks based on vertical specific business rules designed to prevent situations such as emailing the wrong recipient or attaching incorrect content. The out-of-the-box AI and dictionary based classifiers can detect medical, legal, financial, or personal information, as well as social security or credit card numbers, etc.

## 2 Two-factor authentication (2FA) for recipients

Every email sent via ZIVVER requires that the recipient identify themselves via two-factor authentication (2FA). That way, there will never be a doubt that the message reaches the correct individual(s). ZIVVER provides 2FA via a code sent to the recipient mobile phone, via email, or 2FA apps (such as Google authenticator).



## 3 The safest method of email encryption


ZIVVER employs asymmetric email encryption, which consists of two keys to encrypt a message. Secret keys are exchanged over the internet or an intranet network. It ensures that malicious individuals don't get access to the message. It is important to note that anyone with a secret key can decrypt the message, and this is why asymmetrical encryption uses two related keys. A public key is made freely available to anyone who might want to send an email to you. The second private key is kept a secret so that only you and the recipient(s) can read the email.


## 4 File sharing up to 5TB


A unique ZIVVER feature is the ability to send up to 5TB of data as an email attachment. No other service in the world offers such large file sharing capability via an email attachment. As storage solution capabilities increase and data becomes more dense, larger file sharing capacity will be needed. If in the future 5TB file sharing becomes a part of your routine, ZIVVER will have you covered.

Do you have questions about Secure Email or any other ZIVVER feature?


**Please contact our team.**

 +44 (0) 203 285 6300

 [contact@zivver.com](mailto:contact@zivver.com)

 [www.zivver.com](http://www.zivver.com)

 [linkedin.com/company/zivver](https://linkedin.com/company/zivver)

 [@ZIVVER\\_EN](https://twitter.com/ZIVVER_EN)

 [facebook.com/zivver](https://facebook.com/zivver)