

zivver



NIS2 and email security

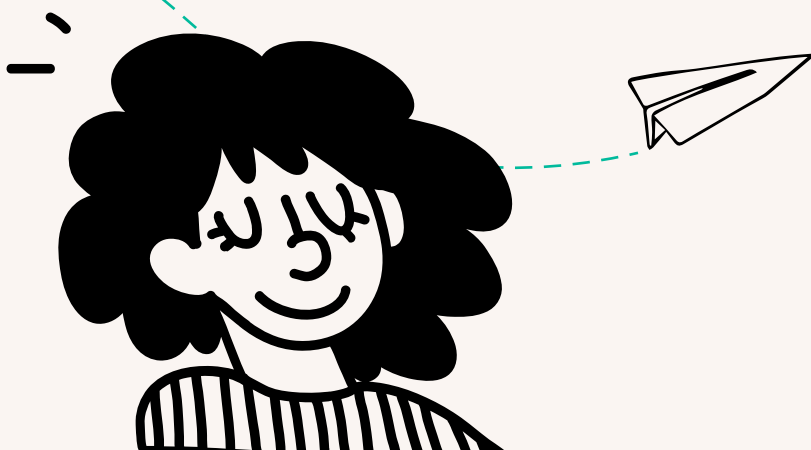
Your checklist
for NIS2 compliance



Introduction

NIS2 sets out stringent practices for protecting data, particularly in the realm of digital communications. Evaluating your existing communications tools to ensure they meet the requirements of NIS2 is a key step to meeting compliance.

This guide will outline everything you need to know to understand your organization's responsibilities around email security under NIS2, including a checklist to help guide you on your way toward NIS2 compliance.



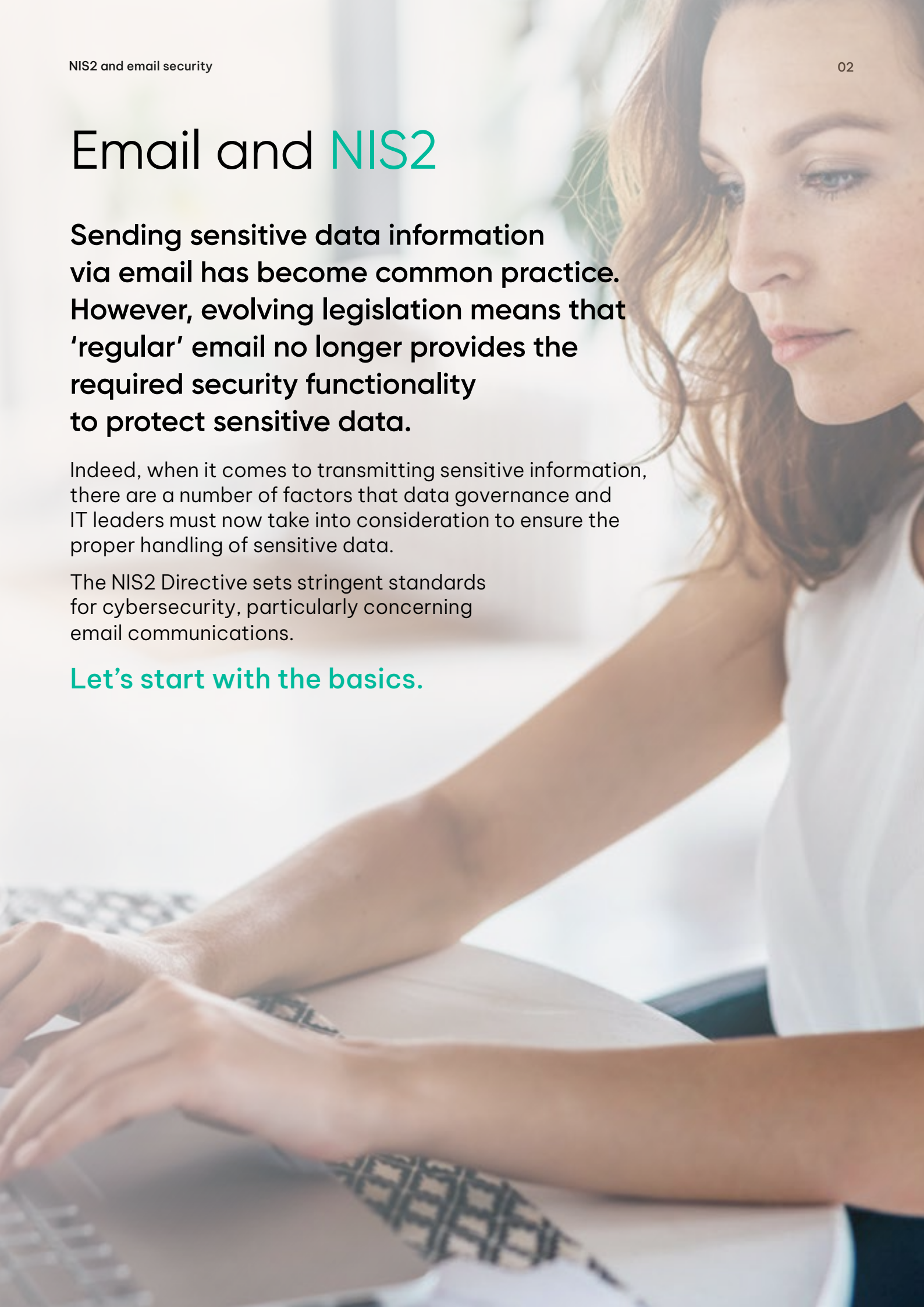
Email and NIS2

Sending sensitive data information via email has become common practice. However, evolving legislation means that 'regular' email no longer provides the required security functionality to protect sensitive data.

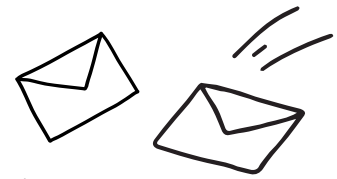
Indeed, when it comes to transmitting sensitive information, there are a number of factors that data governance and IT leaders must now take into consideration to ensure the proper handling of sensitive data.

The NIS2 Directive sets stringent standards for cybersecurity, particularly concerning email communications.

Let's start with the basics.



What is NIS2?



NIS2 stands for Network and Information Security Directive. Introduced in 2020, NIS2 is a continuation and expansion of NIS, the previous EU cybersecurity directive.

NIS2 intends to expand on the original NIS directive. It enhances the security of network and information systems within the EU by requiring operators of critical infrastructure and essential services to implement appropriate security measures and report any incidents to the relevant authorities.

NIS2 enforces more stringent measures across Europe, and expands its EU-wide security requirements and scope of covered organizations and sectors. In this way, NIS2 seeks to improve the security of supply chains and simplify reporting obligations.



Who does NIS2 apply to?

NIS2 affects all entities that provide essential or important services to the European economy and society, including companies and suppliers.

If your organization falls under any of the categories below, NIS2 is applicable to you.

Essential Entities (EE)

Size threshold: varies by sector, but generally:

250
employees

€50 million
Annual turnover OR

balance sheet of
€43 million

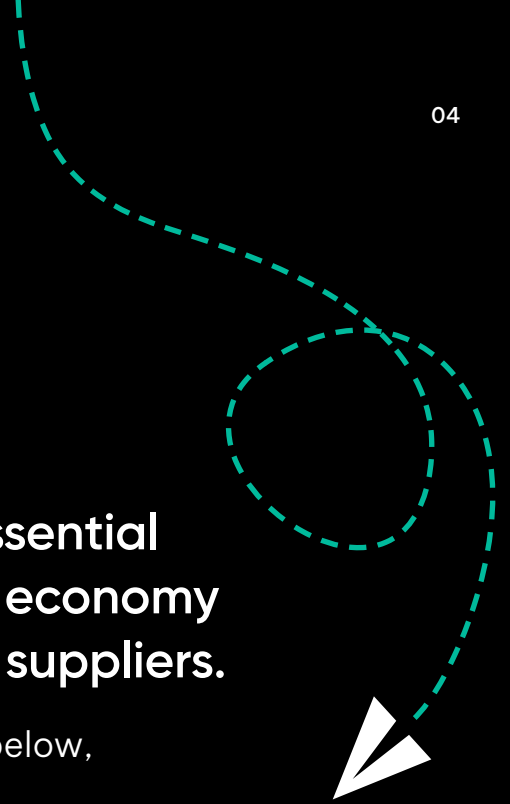
Important Entities (IE)

Size threshold: varies by sector, but generally:

50
employees

€10 million
Annual turnover OR

balance sheet of
€10 million



Essential Entities (EE)



Public Administration



Space



Energy



Health



Finance



Transport



Water Supply
(Drinking & Wastewater)



Digital Infrastructure
E.g. cloud computing service providers and ICT management

Important Entities (IE)



Postal Services



Chemicals



Research



Foods



Waste Management



Digital Providers
E.g. social networks, search engines, online marketplaces



Manufacturing
E.g. medical devices and other equipment Digital Providers

Plus all sectors under “essential entities” and within the size threshold for “important entities”

Important note

An entity may still be considered “essential” or “important” even if it does not meet the size criteria, in specific cases such as when it is the sole provider of a critical service for societal or economic activity in a Member State.

NIS2 applies not only to operators of essential services (OES) and digital service providers (DSPs), but to any

entities that provide services essential for the maintenance of critical societal and economic activities.

NIS2 requires medium to large sized entities within the relevant sectors to take appropriate technical and organisational measures to manage risks posed to their network security and information systems.

Why compliance is vital for your organization

The importance of compliance with NIS2 cannot be overstated. Organizations that fail to take adequate measures to protect their networks and information systems risk not only financial losses but huge reputational damage and legal liabilities. Fines for non-compliance can reach up to 2% of an organization's total annual turnover or €10 million – whichever is greater.

Executives and directors face severe consequences for non-compliance. Under the new regulations, Member States are required to establish legal penalties which can include substantial fines and even criminal charges in some cases. Additionally, executives and directors also face personal liability for any breaches that occur as a result of their failure to implement adequate cybersecurity measures.

In short, the stakes are high. Steps must be taken to comply with the NIS2 directives in order to protect not only their operations and organizational reputation but also the personal liability of leadership teams.



Risk fines from
€10 million



How does NIS2 impact digital communications?

One of the main requirements of the NIS2 guidelines, set out in [Article 21](#), is to have policies and procedures in place regarding the use of encryption and secure communication platforms.

Specifically, NIS2 requires operators of essential services and digital service providers to use multi-factor authentication (MFA) or continuous authentication solutions to ensure data protection.

In addition, [article 24](#) of the directive allows Member States to require essential and important entities to use specific ICT products, services, and processes that are certified under European cybersecurity certification schemes to demonstrate compliance with the requirements of [article 21](#).



How **secure** is email?

It may surprise you to learn that email is inherently insecure. According to research¹, 88% of employees say they rely on email to get their job done and 81% see email as the most secure way to send sensitive information.

However, standard email traffic is not encrypted, meaning that the content of emails can be intercepted and read by third parties. So, for sharing sensitive data, such as medical information, personally identifiable information (PII) or financial data, email requires additional security measures to prevent security incidents.

Limitations of Transport Layer Security (TLS) email security

TLS is a protocol used to encrypt email traffic and improve its security. Unfortunately, TLS is optional and opportunistic, meaning it depends on the settings of sending and receiving email servers. If either server does not support TLS, or if the settings are not configured correctly, the email will be sent unencrypted, putting the privacy and confidentiality of the information at risk.



DANE for proper server control

TLS presents an additional often overlooked problem. While TLS does provide encryption, it does not guarantee that the email will be sent to the correct server. TLS is susceptible to so-called Man-in-the-Middle (MitM) attacks, in which third parties are able to route encrypted emails to another server, instead of the recipient's, without anyone noticing.

Domain Name System-based Authentication of Named Entities (DANE) improves the security of email traffic through proper server control, using DNSSEC (Domain Name System Security Extensions) to verify the authenticity of the email server, and ensures emails are delivered to authorized servers only.

Provided that both the recipient and sender have configured their mail servers correctly, DANE eliminates the risk of emails not being delivered to the right servers. In the Netherlands, only 59% of domain names are secured with DANE and adoption in almost all other countries in the world is considerably lower.²



How multi-factor authentication (MFA) improves email security


While DANE ensures that emails are delivered securely from the sending to the receiving server, it does not protect the email once at rest in the recipient's inbox. After all, any individual with access to a user's mailbox can read the email, including administrators of the email service, the organization, a colleague (if a device is left unattended), or any unauthorized person who has obtained the user's password.

MFA is a familiar protocol for most of us today, used frequently to protect sensitive data in banking applications, healthcare or government portals, or work platforms. MFA provides an extra layer of security that requires users to provide a second form of authentication, such as a unique

code sent to their mobile device, in addition to their password.

While MFA is considered best practice for securing accounts, it is lacking in 'regular' email. NIS2 refers to the application of MFA to ensure only authorized individuals can access sensitive data.

From Secure Email Gateway (SEG) to Email Data Protection (EDP)



Regulations such as NIS2 are prompting IT leaders to evaluate their tools and solutions, presenting an opportunity to identify vulnerabilities and enhance existing tools to combat risk vectors in the organization's digital infrastructure.

As we have made clear, standard email clients, such as Microsoft 365, fall short on a number of security fronts required to meet compliance with NIS2.

For this reason, email must be enhanced with DLP tools and advanced encryption protocols, often in addition to secure email gateways.

Traditional SEGs fail to detect and prevent common human errors, such as sending emails to incorrect recipients - some of the leading causes of data incidents. This is often because SEGs rely on basic filters and rules that do not adequately address simple mistakes.

Moreover, SEGs operate as gateways without user interaction, offering no user-friendly way to warn employees about potential errors, and providing little support in helping users to proactively manage sensitive data securely.

How to email securely and compliantly

Email data protection solutions proffer a number of tools to support compliance, including:

- ✓ Data loss prevention tools
- ✓ Large file transfer capabilities
- ✓ Advanced encryption
- ✓ 2FA controls
- ✓ Recall and revocation tools
- ✓ Security automation functionality

...and more.

EDPs empower users to utilize the right security levels at the right time through the application of strong encryption and 2FA, ensuring the confidentiality and integrity of data.

Seven steps to NIS2 compliance

To guide you along the path to NIS2 compliance, we have provided a checklist to support you in taking the necessary steps to enhance your email security. From advanced encryption to data loss prevention, we're ready to support your organization in meeting the requirements of NIS2.

1. Implement robust encryption protocols

Encryption is a cornerstone of NIS2 compliance. According to Article 21 of the NIS2 Directive, policies and procedures regarding the use of cryptography including, where appropriate, encryption, are required. While Microsoft 365 (M365) supports transport encryption through TLS, integrating DNS-based Authentication of Named Entities (DANE) can enhance security.

M365's DANE implementation, however, lacks fallback mechanisms, making supplementary encryption solutions necessary.

Actions

- 1 Enable TLS for all email communications
- 2 Implement DANE for domain-level encryption
- 3 Use supplementary encryption tools to provide fallback mechanisms

How Zivver can help

Zivver provides advanced encryption protocols for email and file transfers, ensuring that sensitive information remains protected from unauthorized access during transmission and storage.



2. Enforce multi-factor authentication (MFA)

MFA is critical in preventing unauthorized access to data. In addition to encryption, Article 21 of the NIS2 Directive specifies the use of multi-factor authentication.

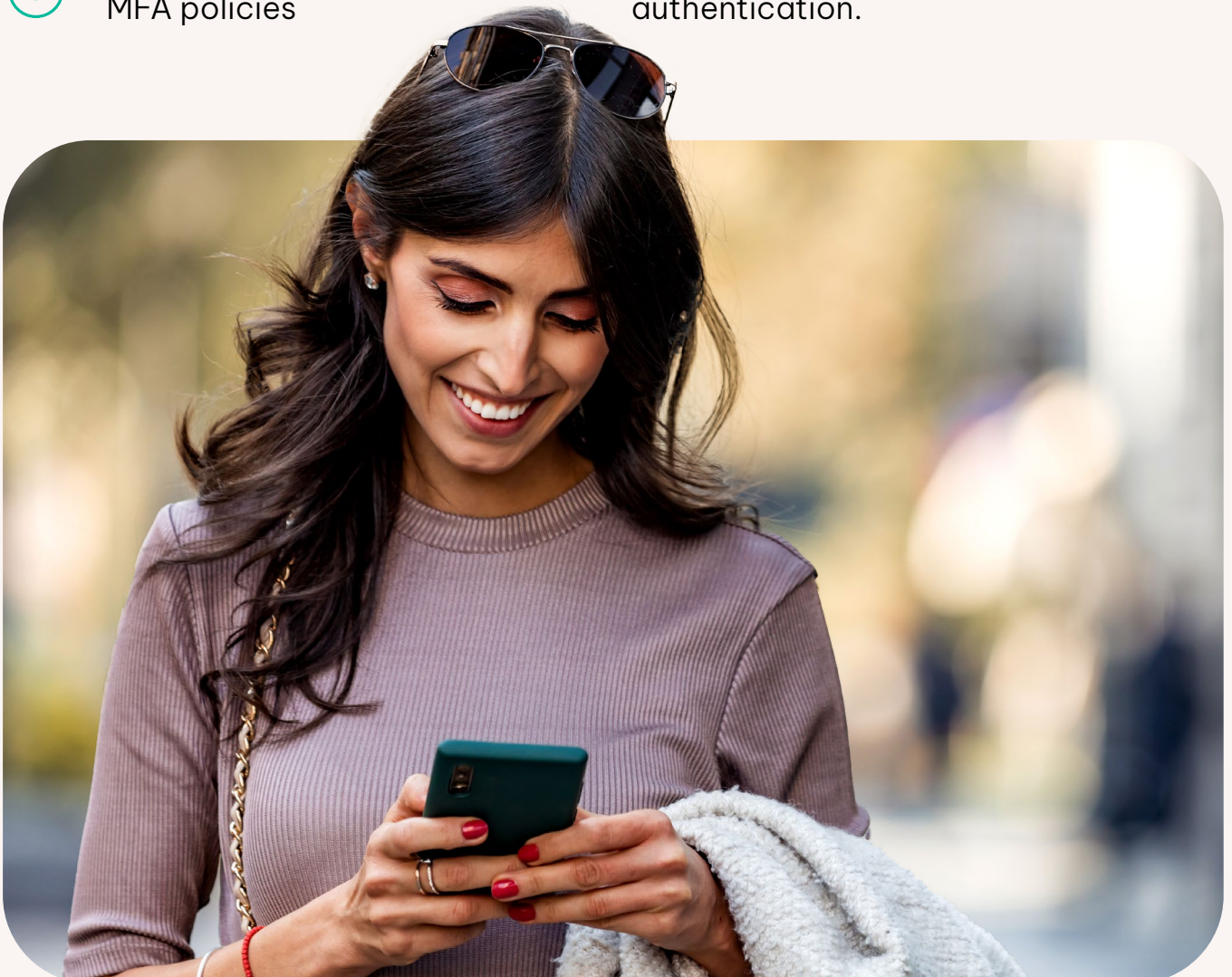
While M365 supports MFA, it is limited in scope. Implementing MFA for both internal and external recipients ensures comprehensive protection.

Actions

- 1 Enable MFA for all users within M365
- 2 Integrate third-party MFA solutions for external recipients
- 3 Regularly review and update MFA policies

How Zivver can help

Zivver integrates MFA into email, enhancing the security of user access to sensitive communications, with flexible authentication methods for third-party recipients including SMS codes, passwords, or email authentication.



3. Automatic email classification and data loss prevention (DLP)

Effective data classification and data loss prevention protocols are vital to protecting your data. The NIS2 Directive emphasizes the importance of approved data classification and appropriate protection measures. M365's native tools for email classification and DLP are often inadequate for NIS2 standards, necessitating advanced classification tools.

Actions

- 1 Set up automatic classification rules in M365
- 2 Integrate advanced DLP solutions that go beyond keyword matching
- 3 Conduct regular audits of classification and DLP policies

How Zivver can help

Zivver's data loss prevention features help organizations avoid the accidental or malicious sharing of sensitive information. Zivver integrates advanced DLP solutions that go beyond keyword matching, aligning with NIS2's focus on preventing cybersecurity incidents that could disrupt critical infrastructure operations.

4. Secure handling of sensitive attachments

Attachment security is crucial. M365 limits encrypted attachments to 25MB, which may not be sufficient for all needs. Consider supplementary solutions for handling larger files securely.

Actions

- 1 Use Purview Message Encryption for attachments up to 25MB
- 2 Implement integrated secure file transfer solutions for larger attachments
- 3 Ensure all attachments are scanned for sensitive information before sending

How Zivver can help

Zivver integrates with email clients to enable secure large file sharing, up to 5TB. No more switching to third party platforms!



5. Prevent human error

Human error is a leading cause of data breaches. Misaddressed emails, one of the most common causes of data loss globally, can lead to significant data leaks. Article 21 of the NIS2 Directive stresses the importance of procedures to prevent such mistakes.

Actions

- 1 Use email verification tools to confirm recipient addresses
- 2 Integrate solutions that prompt users to verify sensitive information before sending
- 3 Train employees regularly on the importance of email security

How Zivver can help

Arm people with tools to prevent data loss in the moment it matters. Zivver integrates seamlessly with email and notifies users in the moment a mistake is about to happen, so they can take action to revoke sensitive data, encrypt their email before sending, or correct recipients in the 'to' or 'bcc' fields.

6. Revocation and tracking of emails

The ability to revoke access to and track emails is important for compliance. While M365 allows message revocation through Purview Advanced Message Encryption, it is limited to recipients outside the Microsoft ecosystem.

Actions

- 1 Enable message revocation within M365 where possible
- 2 Use supplementary tools that allow for broader message revocation capabilities
- 3 Implement tracking systems to monitor the delivery and opening of sensitive emails

How Zivver can help

Zivver enables recall emails without limits, and provides insights into the status of emails including whether they have been opened. This means users can navigate potential data incidents and take action accordingly.

7. Regular security audits and updates

Regular audits ensure continuous compliance. Article 21 of the NIS2 Directive requires ongoing monitoring and updates to security protocols.

Actions

- 1 Schedule regular security audits of your email systems
- 2 Update security protocols and tools in response to new threats and regulations
- 3 Keep documentation of all compliance measures and audits for regulatory review

How Zivver can help

Zivver provides auditing and logging capabilities, allowing organizations to track and report on communication activities. Zivver can help with regular audits of email systems, updates to security protocols in response to new threats, and support in documentation of compliance measures.



Conclusion

Traditional email falls short when it comes to securely handling sensitive data. The introduction of NIS2 increases the responsibilities of organizations to take action and enhance tools to ensure they are robust enough to protect sensitive information.

It's time to take action; compliance is no longer about ticking a box and doing just enough to get by. The data protection landscape is changing, offering organizations an opportunity to leverage data governance as a competitive advantage in the marketplace.

By following our seven steps, organizations can ensure their email communications are secure and compliant, mitigating risks and enhancing their overall cybersecurity posture.



What next?

We take the complexity out of compliance.

Zivver is the email security solution that prevents data loss and supports compliance in Microsoft 365, Outlook and Gmail.

Adaptable, user-friendly, and powered by contextual machine learning, Zivver integrates with email clients to stop the leading causes of data leaks. Our suite of email security tools empower users to share sensitive data by email safely and with confidence, with unparalleled encryption and human error prevention tools.

Find out how we can help your organization to comply with NIS2.



zivver

Secure email.
Effortless compliance.



contact@zivver.com



+44 (0) 203 285 6300