mailguard

FUTURE PROOF

EMAIL SECURITY SOLUTIONS

WHITEPAPER

ARE YOU GDPR READY?

FUTURE PROOF YOUR EMAIL SECURITY FOR GDPR

WHAT IS THE GENERAL DATA PROTECTION REGULATION (GDPR)?

On 25 May 2018 a new regulation enforced by the European Union (EU) comes into effect: the General Data Protection Regulation (GDPR). The GDPR aims to protect the personal data of EU residents, including anyone physically residing in the EU, even if they are not EU citizens.

The GDPR extends due diligence obligations and potential liability to both data controllers and data processors. This means the regulations will impact all aspects of business and organisational operations—most importantly the way your company manages, protects and secures its data (including email).

Most significant is the enforced mandatory reporting of data breaches. Failure to comply with the regulation by not reporting a data breach to the eu will result in hefty fines and company losses: up to €20 million or 4% of total worldwide annual turnover of the preceding year (whichever is higher). Even if your company is not physically based in the eu, and you haven't had to comply with eu data privacy laws before, chances are the gdpr will affect your company's approach to data privacy and email security wherever you're based in the world.

GDPR HIGHLIGHTS	
FINES	A tiered approach applies, with the level of fine dependent on the category of obligation breached. Non-compliant companies could receive fines of up 4% of their annual worldwide turnover or €20 million.
TERRITORIAL BOUNDARIES	Your company no longer has to be based or established in the EU to be subject to the European data protection rules. If you offer (free or paid) goods and services to EU citizens or monitor their behaviour, you will be subject to the GDPR.
CONSENT	Rules around consent to use personal data have been dramatically strengthened, e.g. pre-checked tick boxes consenting to subscribe to a mailing list is no longer acceptable.
YOUR DATA RIGHTS	The right to erasure/right to be forgotten: GDPR allows data subjects (individuals) to require data controllers to: (i) erase their personal data; (ii) stop any further use or sharing of their data; and (iii) stop third parties from processing their data.
DATA BREACHES	If there is a data breach, your company must notify the relevant Information Commissioner Office within 72 hours of first becoming aware of the breach. If the breach leads to the loss of highly sensitive data, posing a high risk to data subjects, the company must also notify the individual data subjects impacted.

MailGuard Pty Ltd Detecting and blocking fast-breaking, criminal intent email threats 2-48 hrs ahead of the market
198 Normanby Rd, Southbank VIC Australia 3006 | Phone: +61 3 9694 4444 Fax: +61 3 9011 6144 | info@mailguard.com.au

mailguard

HOW DOES GDPR AFFECT MY COMPANY'S DATA AND EMAIL SECURITY?

From a cybersecurity perspective, full compliance with GDPR will require dedicated resourcing and technical support. You may need to apply significant changes to your company's data collection policies and procedures, as well as investments in new and effective cybersecurity tools to ensure your company data is safe from potential hacking and data breaches.

GDPR is a wake-up call for all c-level executives, information security, technology, and risk and compliance managers. No matter if you're an international corporation trading from within the EU, or an Australian-based SMB with customers located in Europe, as of 25 May 2018 you will be under the auspice of GDPR regulations and liable for its hefty penalties for failing to report data breaches.

GDPR regulations and data breaches: key threats, opportunities and risks

Ways the GDPR regulations may affect your company's approach to email security:

- Highlight the technological cybersecurity skill gaps.
- Being left behind and/or lack of understanding in fast-moving cybersecurity trends.
- Inability to cope with increasing and targeted cyberattacks by cybercriminals through malicious email scams.
- Your competitors using stronger data privacy and cybersecurity solutions as a marketing advantage.
- Even if your own company's email security is robust, your third-party suppliers, contractors and vendors are still vulnerable and may allow malware to access and infiltrate your organisational data.

Once a data breach has occurred your company may endure:

- Hefty GDPR fines and penalties, which may result in irreversible financial stress.
- Loss of customers and hence business viability. 70% of customers would leave a company following a data breach.
- Damage to your brand reputation and share price through GDPR and media reporting.
- Loss of employees and destruction of company culture and goodwill.
- Tarnished professional reputations and loss of C-level executive status.

MailGuard Pty Ltd Detecting and blocking fast-breaking, criminal intent email threats 2-48 hrs ahead of the market
198 Normanby Rd, Southbank VIC Australia 3006 | Phone: +61 3 9694 4444 Fax: +61 3 9011 6144 | info@mailguard.com.au

WHAT DO I NEED TO DO TO ENSURE MY COMPANY'S EMAIL SECURITY IS GDPR READY?

Approximately 91% of all corporate cybercrime is initiated by email. It's the method of attack favoured by cybercriminals, deceiving employees into clicking on malicious email links that collect login credentials and expose company data.

Email is the largest cyber threat vector and may not be clearly understood and/or it may be underestimated within your company.

ONE Begin a discussion in your company about the impact of cybercrime

Many large corporate data breaches are not caused by hacking but the result of human vulnerabilities exploited through email—such as 'phishing' attacks, malicious attachments and CEO fraud. Educating your C-level executive team, board, and workforce is vital to counteracting any cyber breaches that will expose your company to GDPR fines.

Businesses today are losing millions of dollars to cyberattacks that could have been easily prevented

A common misconception is that cybersecurity is seen as an IT issue alone, with CEOs defaulting full responsibility to their IT departments. As GDPR regulations and compliance highlight, cybersecurity isn't that simple. Good cybersecurity starts with the leaders at the top of your organisation, and good management must include commitment from all levels of company governance and employees.

According to the *World Economic Forum 2018 Global Risks Report*, more than 4 billion data records were reported stolen from businesses in 2016 alone—more than during the previous two years combined. Talk to your internal communications team about implementing an awareness campaign around the dangers of malicious email attacks. MailGuard offers free educational resources to help businesses educate their employees about the growing risks of cybercrime.

MailGuard Pty Ltd Detecting and blocking fast-breaking, criminal intent email threats 2-48 hrs ahead of the market
198 Normanby Rd, Southbank VIC Australia 3006 | Phone: +61 3 9694 4444 Fax: +61 3 9011 6144 | info@mailguard.com.au

TWO Commence a cybersecurity data audit

Find out what data your company is collecting and how it is stored

What information does your company handle that could create a liability under the GDPR? Ensure your audit scans all technological platforms and devices. Is there company data held by contractors and other third parties? If so, what actions have they taken to ensure this data is protected?

Identify what data you already have

Look at all kinds of assets stored in all formats. List your data assets in categories to make it easier to assess e.g. CRM platforms, POS purchase information, online shopping records, analytics data, marketing lists, social media contacts. Once you have established a clear picture of your company's data management processes, and the data you have access to, you are in a position to make a risk assessment and gap analysis.

THREE Undertake a cybersecurity risk assessment

Ask questions to identify your level of risk

What cyber threats could your company face? Where are the security weak-points in your technology infrastructure? Do you have effective cybersecurity measures in place? What threats does your security software protect you from? Do you have education programs in place to counteract human security vulnerabilities? How would you know if your data was compromised? What is your responsibility to third parties whose data you handle? Who is responsible for your company's cybersecurity management?

Use answers to these questions to identify the gaps in your cybersecurity plans and measure vulnerabilities to your company.

GET YOUR FREE GDPR READINESS CHECKLISTS

Contact us for:

- an obligation-free GDPR email security readiness consulation
- GDPR readiness checklists for data controllers and processors

GET FUTURE PROOF
mailguard.com.au/future-proof

MailGuard Pty Ltd Detecting and blocking fast-breaking, criminal intent email threats 2-48 hrs ahead of the market
198 Normanby Rd, Southbank VIC Australia 3006 | Phone: +61 3 9694 4444 Fax: +61 3 9011 6144 | info@mailguard.com.au

mailguard

FOUR Review and update your data privacy policies and procedures, including email

Revisit all your policies relating to data protection and privacy

This includes the collection and retention of email content. Accurate and regularly updated policies written in plain English is key to keeping your customers informed about how their personal information is collected and handled, and achieving compliance with GDPR.

These policies are not just about ticking the GDPR legal requirement box — they help establish company and brand trust for effective management of existing and potential customer relationships. For this reason they should be written in clear and concise language, with updates communicated to all customers via email and other digital channels including social media and your website.

Policies affected may include, but not be limited to: data protection policy, privacy notice, data protection impact assessment (DPIA) procedure, records retention policy, data subject rights policies, international transfer policy, data protection officer (DPO) policy, staff training policy, information security policy.

FIVE Develop and enact your GDPR cybersecurity implementation plan

Initiating greater accountability and transparency in data management is only half of the formula for GDPR preparation. Developing a solid implementation plan containing an overview of technology systems and solutions, scope, stakeholders, major tasks, and required resourcing to support the implementation process (such as budget, hardware, software, facilities, staffing), and site-specific implementation requirements may fall under an implementation plan for your company.

MailGuard Pty Ltd Detecting and blocking fast-breaking, criminal intent email threats 2-48 hrs ahead of the market
198 Normanby Rd, Southbank VIC Australia 3006 | Phone: +61 3 9694 4444 Fax: +61 3 9011 6144 | info@mailguard.com.au

GDPR RISKS, OPPORTUNITIES & THREATS

WAYS THE GDPR REGULATIONS MAY AFFECT YOUR COMPANY'S APPROACH TO EMAIL SECURITY

- Highlight the technological cybersecurity skill gaps.
- Being left behind and/or lack of understanding in fast-moving cybersecurity trends.
- Inability to cope with increasing and targeted cyberattacks by cybercriminals through malicious email scams.
- Your competitors using stronger data privacy and cybersecurity solutions as a marketing advantage.
- Even if your own company's email security is robust, your third-party suppliers, contractors and vendors are still vulnerable and may allow malware to access and infiltrate your organisational data

Detrimental effects you company may endure after a data breach has occurred

- Hefty GDPR fines and penalties, which may result in irreversible financial stress.
- Loss of customers and hence business viability. 70% of customers would leave a company following a data breach.
- Damage to your brand reputation and share price through GDPR and media reporting.
- Loss of employees and destruction of company culture and goodwill.
- Tarnished professional reputations and loss of C-level executive status.

We view the introduction of the GDPR Scheme as an essential contribution to global cybersecurity

With mounting pressure on governments to do more to close cybersecurity gaps, higher standards for data and privacy compliance will be adopted by companies globally.

Forward-thinking business owners and CXOs who take action now to increase their level of cybersecurity will be better-positioned to future-proof their company from the risks of data breaches and GDPR non-compliance.

MailGuard is committed to supporting businesses who take the initiative to protect themselves from cybersecurity vulnerabilities. With tangible GDPR transparency measures now in place in the event of a data breach, multi-layered email security protection is critical to the future health of your company.

Contact us for an obligation-free email security consultation and GDPR readiness checklists for data controllers & processors:
mailguard.com.au/future-proof

MailGuard Pty Ltd Detecting and blocking fast-breaking, criminal intent email threats 2-48 hrs ahead of the market
198 Normanby Rd, Southbank VIC Australia 3006 | Phone: +61 3 9694 4444 Fax: +61 3 9011 6144 | info@mailguard.com.au

mailguard

MailGuard Pty Ltd

mailguard.com.au/future-proof

GENERAL ENQUIRIES
Phone +61 3 9694 4444

SALES
1300 30 44 30
expert@mailguard.com.au

TECHNICAL SUPPORT
Australia 1300 30 65 10
United States 888 848 2822
United Kingdom 0 800 404 8993

HEAD OFFICE
MailGuard Pty Ltd
198 Normanby Rd
Southbank VIC Australia 3006
Phone +61 3 9694 4444
Fax +61 3 9011 6144
Email info@mailguard.com.au

REGISTERED BILLING OFFICE
MailGuard Pty Ltd
68-72 York St
South Melbourne VIC Australia 3205