NZ Privacy Laws are changing

Is your Employee Email System going to comply in terms of privacy and data storage? Are you ready for these changes?

Get ready for the upcoming privacy law changes

The Privacy Bill is making its way through Parliament and will likely become law in 2020. The Government is updating New Zealand's Privacy Act 1993 to make sure personal information is kept safe and secure in line with new technology and ways of doing business. In particular, the reforms aim to encourage private and public sector agencies to identify risks and prevent incidents that could cause harm. Reform proposals include stronger powers for the Privacy Commissioner, mandatory reporting of privacy breaches, new offences and increased fines. Even your everyday employee email system will need to comply.

GDPR & The Privacy Act

The General Data Protection Regulation (GDPR) is already paving the way for a new international standard of data management and email marketing for everyone - not just EU citizens. While we may not think of email as subject to national or International privacy laws, your mailbox in fact contains a trove of personal data. From names and email addresses to attachments and conversations about people, all are covered by the GDPR's strict new requirements on data protection, and will almost certainly be covered under the updates to New Zealand's Privacy Act.

Acts worldwide are about protecting data that is stored or sent. Employee email could be majorly impacted if sensitive data is sent in an employee email or from an employee to someone and that information was used to breach data held by the employer. So employee email needs to be managed with greater emphasis on security, risk and compliance - it needs to be easily audited to measure these attributes. Don't risk a breach of your data.

You can review the NZ PRIVACY ACT here, and find what the GDPR website advises for your everyday emails here.

Penalties

The penalties for data breaches are very real. Only last year British Airways was fined $328 million dollars under the new GDPR data protection rules. Check out the article here. It can take years to cultivate a good reputation for your business and yet this can be undone in a flash. It is certainly worth putting all practicable measures in place to ensure the security of your email systems.

Privacy Commission Advice - here's how to be better prepared...

- Email Security measures - ensure you are using a system that allows for TLS, DKIM and DMARC so that your messages can't be spoofed or altered and the recipient server recognises them as genuine. You don't need to understand or implement these measures yourself, use C9 Signature and it will all be taken care of.
- Ninety-one percent of cyber attacks begin with a phishing email, in which hackers attempt to gain access to an account or device using deception or malware. Links and attachments from unknown accounts should never be clicked or downloaded (source: gdpr.eu).
- 60 per cent of complaints to the Office of the Privacy Commissioner are from people denied access to their information. If a customer or employee requests their information, you are required to respond to that request within 20 working days. Make sure you have a process in place to handle customer requests for information held about them if, and when, they are made.
- Make sure you hold and use personal information in a safe and secure way and dispose of it securely when you have finished with it.
- If you use an overseas-based service provider, like cloud software, ask the provider how they're meeting New Zealand privacy laws.
- Appoint a privacy officer. Every business should have a privacy officer, according to the Privacy Act. This is someone who has a general understanding of the Act and can deal with privacy issues when they arise.

Action Items - where do you start?

It's important to make sure your emails are security compliant. This might include compliance to the GDPR standard and the NZ Privacy Act, however It's equally important that you apply DKIM, SPF and DMARC. These are all standards that you should be supporting, especially if you don't want your emails to be identified as potential spam.

Trying to understand these complex requirements is a daunting prospect and can cost a great deal of time and money in consulting, software and implementation. Using C9 Signature you can achieve the most up-to-date level of security around your email and your domain. This reduces your risk and enables you to meet your compliance, security and auditability obligations.

c9signature What is it and how will it help reduce your risk?

- C9 Signature is a secure, third-party server with the highest levels of security, traceability and reporting. In addition, your employee emails are seamlessly branded and tracked with dynamic templates and disclaimers.
- You do not need to alter the way you send and receive your emails - continue to use your current current Office 365, GSuite or Exchange environments and the emails are simply routed through our secure system before they reach the end recipient.
- Compliance - We employ DKIM which shows the recipient server that the message hasn't been altered.
- SPF - when you're passing email through C9 Signature, it's possible to prevent emails from spoofing your domain. Provided your SPF is set to hard fail messages from unrecognised sending servers, then nobody can set up a copycat account.We use opportunistic TLS meaning that the email is sent over a secure line.
- Visibility – if authorised, administrators can access the original email and see all information related to the message, including the headers. C9 Signatures built-in search function means messages are easy to find, ensuring traceability is achieved with the greatest simplicity.
- You can see who a message was delivered to, at what time, and to what server, allowing you to meet data obligations.
- Data security - if requested, we can instantly delete content from our server after it has been delivered.
- Access to the information – we can restrict the level of access available to administrators to different levels.

- Reporting Interface - you can easily see the level of interaction with your emails, and any concerning patterns e.g. employees mass forwarding emails.
- This GUI is user-friendly and tracks all third-party interaction with email, rather than just a simple Office 365 or Gmail report on what you have sent and received.
- If malware activity is detected then we can isolate the sender or sending server / domain and prevent mail delivery for as long as necessary.
- Administrators can build rules to react to triggers such as specific words, subject lines, attachments and force the message to be dropped or returned to sender.
- Disclosure statements – you can prove that a link was transmitted and if it has been clicked on.
- Read receipts – we can silently notify your users of the exact time an email has been opened without the recipient being aware. You can set up a rule so that receipts go into a folder and you don't need to see them unless you need to check something.

C9 Signature is easy to deploy either as a hosted service, or within your own email environment. It can connect to your active directory and you continue to use your current email platform, be it Outlook, Gmail or something else, as we integrate with what currently exists. It is also inexpensive. Contact us today and we can help you meet these new data obligations.

www.cumulo9.com

CONTACT US

Cumulo9, one of New Zealand's leading email service providers has developed C9 Signature, used by leading businesses to mitigate their risks, comply with their data obligations and stay out of the headlines.

cumulo9
Digital Communications Transformed