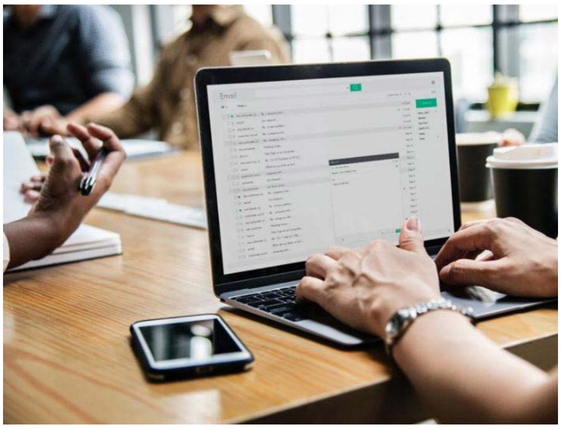
C9 Signature

Does your Employee Email System comply in terms of privacy, data storage and security?

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. 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. The NZ Privacy Act is currently being updated and will also be addressing data responsibilities.

Reduce your risk with C9 Signature



- 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.