ALSO AN EMAIL CONVERSATION

LET'S START WITH A QUESTION. A REALLY SIMPLE ONE.
"HOW DO YOU EMAIL?"
AND HERE'S ANOTHER.
"WHO DO YOU EMAIL?"

stayprivate.com

ALSO AN EMAIL CONVERSATION

Let's start with a question. A really simple one.
"How do you email?"
And here's another.
"Who do you email?"

The reality is, the How & Who of emailing has actually become one of those 'Simple-Difficult' questions for companies. Because the follow-up question this year has become:

"Is your company's email process GDPR-compliant?"

Most company and department heads would likely hesitate at this, fudge an opaque answer like, "We're very aware of GDPR; rest assured we're taking all the appropriate measures", and then having bought some time, fire off an email to their CTO, IT department, or recently-appointed Data Protection Officer.

Compose. Subject: GDPR – Email? WTF? Send.

The fact is: GDPR is coming. May 25 is the deadline. In regards 'All things data-related', companies have likely been discussing and evaluating and auditing for the last 12 months or more. 2018 is 'The Year of GDPR' and the year 'data' becomes a hot, even incendiary, topic. How data is stored, how it's depersonalised, how customers give permission to be contacted – this is all part of GDPR and new governing legislation where the responsibility lies at the company's door when it comes to compliant conduct and 'digital duty of care'.

'Consent' dominated the early days of the GDPR conversation. This typically led to companies appointing task forces and action groups and beginning an audit process. The thought of an audit may have sounded slightly painful at the time, but also like a necessary evil in order to answer more of those Simple-Difficult questions. You can imagine the sort. Who, what, where, how questions like…

- Can we map out what we do with our data and how we process it?
- Do we know where all our data comes from? The sources? The feeds? The platforms?

"Consent' dominated the early days of the GDPR conversation. This typically led to companies appointing task forces and action groups and beginning an audit process."

ALSO AN EMAIL CONVERSATION

- Is our legacy data joined-up and still relevant?
- Do we know everyone who has access to all our data?
- Just where exactly does it live, where does it go, and what are we doing with it?

All good questions, but where even good answers cannot provide the whole GDPR solution – because in the looming shadow of GDPR, one boardroom agenda point still lurks unaddressed. Email.

You see, GDPR is also an email conversation, and up until now, companies haven't been presented with a GDPR-compliant option. 'Email' has been the White Elephant sitting on the boardroom table, forcing everyone to tilt and lean and crane their necks. Because GDPR is all about data flow. Which means it's inclusive of digital communication and the protocols that keep the flow of data (such as emails) safe and secure and appropriately encrypted.

And the simple fact is, 'email by default' is not secure.

If you're a large enterprise business, emailing internally, colleague-to-colleague, then GDPR doesn't have a bearing – but platforms like Gmail, Hotmail and Outlook aren't sufficiently encrypted, and how many companies never have to email to a client or customer's webmail account?

The moment a company emails outside its network, it's effectively throwing loaded dice. In fact, the odds aren't even that good. Let's consider a few odds. Winning the National Lottery? You're looking at 1 in 14 million. The odds of being in a plane crash? That'll be 1 in 11 million. Whereas… the odds on your email being hacked? It's 1 in 4.

'Email by default' is just way too hackable and leaky. Email hacks happens all the time, and many of us are getting hacked and don't even know it. Back in December 2016, Yahoo stumbled on a 3-year security breach where hackers had accessed and stolen data from 1 billion email user accounts. And the moment a hacker is cruising around your InBox, it's Open Season. They have their hands on your online life.

“The moment a company emails outside its network, it's effectively throwing loaded dice. In fact, the odds aren't even that good.”

ALSO AN EMAIL CONVERSATION

Think in terms of having access to… your online bank account; your LinkedIn, Twitter and Facebook accounts; your cloud services like Google Drive and Dropbox; your streaming accounts like Amazon Prime and Netflix; your online retail purchases on Amazon, iTunes and… everywhere else.

For a hacker, access to your email is access to your life and to your finances – and it's for all the aforementioned reasons that GDPR is a force for corporate change in how companies email.
Certainly "Having a portal" is part of the solution, but not all email exchanges will take place within a portal. That's just not the way people behave or email, and they're not about to abandon their InBox or email address and exclusively communicate through a series of company portals. For most people, 'portals' are a hassle and just another layer of digital admin.
People don't want to stop emailing, or being emailed - but they do want 'Safe Email'. They want 'Email by Design'. Not 'Email by Default'. From the corporate side of this fence, that posed a big headache and an equally big budget response.

Or at least, that was the case up until now.

> "People don't want to stop emailing, or being emailed - but they do want 'Safe Email'. They want 'Email by Design'."

STAY PRIVATE

ABOUT US

StayPrivate ensures safe and secure 2-way communication between businesses and external contacts. Our plug-and-play solution is compatible with all email accounts, making it incredibly easy to encrypt emails and share files securely.

With click-and-PIN access, TLS connections, AES-256 encryption and multi-factor authentication, StayPrivate enables companies of any size to send and receive personal data in a GDPR-compliant manner.

GET IN TOUCH

+44 (0) 20 7101 5000 | sales@stayprivate.com | www.stayprivate.com