CheckRecipient & GDPR
Data Breach Preparation and Prevention in a Rapidly Changing Landscape
CheckRecipient

Key Summary

- Misaddressed emails were the number one form of digital data security incident reported to the Information Commissioner’s Office (ICO) in Q3 2016
- When introduced, GDPR will force organisations to report all personal data breaches to the appropriate governing body (this will be the ICO for the UK) and maintain a register of these internally
- Fines for the worst breaches will rise to up to 4% of an organisation’s past year’s global turnover
- CheckRecipient can help organisations by automatically preventing misaddressed emails and creating an audit log to allow organisations to demonstrate diligence to clients and regulators

An Introduction to GDPR

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>European Commission publishes legislative proposal</td>
<td>Separate negotiations within the council and European parliament are held</td>
<td>European parliament reaches agreement</td>
<td>Negotiations and approval among the three institutions</td>
<td>Regulation is published in the official journal</td>
<td>Two year implementation phase</td>
</tr>
</tbody>
</table>

Figure 1 – GDPR timeline (DLA Piper, 2016)

January 2016 - Draft GDPR released by European Commission to replace the Data Protection Directive (DPD)
- DPD was created to "regulate the collection and use of personal data within the EU"
- GDPR was created to "harmonise differing data protection laws" within the EU
- GDPR is a "Regulation" rather than a "Directive"
  - There is no need to nationally implement this legislation - it is now directly applicable to all EU member states

Key Changes to Current Data Protection Legislation

Increased Fines & Penalties

- Fines of up to 4% of annual turnover for non-compliance, thereby having the highest possible penalties alongside anti-bribery and anti-trust laws
- Fines of up to €10,000,000 or 2% of annual worldwide turnover for failure to comply with breach notification - for potentially both the controller and the processor
- Fines of up to €20,000,000 or 4% of annual worldwide turnover are often triggered through other non-compliance that is alerted to supervisory authorities during a data breach
- Prosecution and potential prison sentences for deliberate breaches of GDPR (IT Governance, 2016)
Mandatory Reporting

- **Article 32** - requirement for controllers to implement appropriate technical and organisational measures alongside a process of frequent testing, evaluating and assessing the effectiveness of each of these measures - burying your head in the sand is no longer an option!
- **Article 33(1)** - notification to supervisory authority "without undue delay, and where feasible, not later than 72 hours after having become aware of it"
- **Article 33(2)** - notification from processor to controller "without undue delay having become aware of the breach"
- **Article 33(5)** - record of every single data breach must be kept, whether or not they are notified and this is permitted for audit by the supervisory of authority
- **Article 34** - notification to individuals if containing information with high risk to rights and freedoms "without undue delay"

GDPR & Misaddressed Emails

Email continues to be the major artery of communication for organisations and one via which highly sensitive information and personal information travels through.

According to recent statistics, misaddressed emails are the most common form of digital data security incident reported to the ICO. This iners that, under GDPR, an organisation is most likely to suffer a fine or penalty due to data loss through a misaddressed email. Some notable examples of penalties issued by the ICO for misaddressed emails from the past 12 months include 56 Dean Street Clinic who were fined £180,000 for inadvertently...
disclosing the identities of HIV positive patients and also Dyfed-Powys Police who were fined £150,000 for inadvertently disclosing the identities of registered sex offenders to a member of the public.

Under GDPR, organisations will have an obligation to report misaddressed emails to the ICO and face fines of up to 4% of global turnover depending on the severity of the breach. Given that misaddressed emails are the number one type of data security incident currently reported to the ICO, this should be of significant concern for all organisations in the transitioning years toward GDPR.

**How Can CheckRecipient Help?**

CheckRecipient is a next generation email security platform which uses machine learning to automatically detect when emails are being sent to the wrong person, allowing organisations to both prevent information being sent to the wrong person and crucially, retain an audit log of warning messages shown to users when sending emails and the response that the user made on the warning that was shown.

The audit feature and preventative nature of CR aligns with the GDPR requirement to "to implement appropriate technical and organisational measures together with a process for regularly testing, assessing and evaluating the effectiveness of those measures to ensure the security of processing" (Article 32).

Furthermore, with increasing numbers of firms adopting CheckRecipient's technology and their role in helping advising other companies in their transition to GDPR, simply relying on staff being as careful as possible and internal training, becomes an untenable posture when protecting personal data.
References


About CheckRecipient

CheckRecipient is a next-generation email security technology to prevent highly sensitive information being sent to the wrong people. CheckRecipient uses artificial intelligence and machine learning to analyse historical email data and automatically identify anomalies and mistakes on outgoing emails which may result in inadvertent data loss. Some of the world’s largest organisations rely on CheckRecipient’s technology across the financial, legal, professional services and biotech sectors. The company is headquartered in London, UK.

Contact Us

contact@checkrecipient.com
+44 2032 879 756
www.checkrecipient.com