Sharing data safely

As the demands to share data grow, so too do compliance risks. New privacy laws make organizations directly liable for data breaches, many of which involve avoidable human error.

We now have a better understanding of the role of proper data handling in preventing data breaches. Janusnet solutions can help you share data safely.

The growing pressure to share data

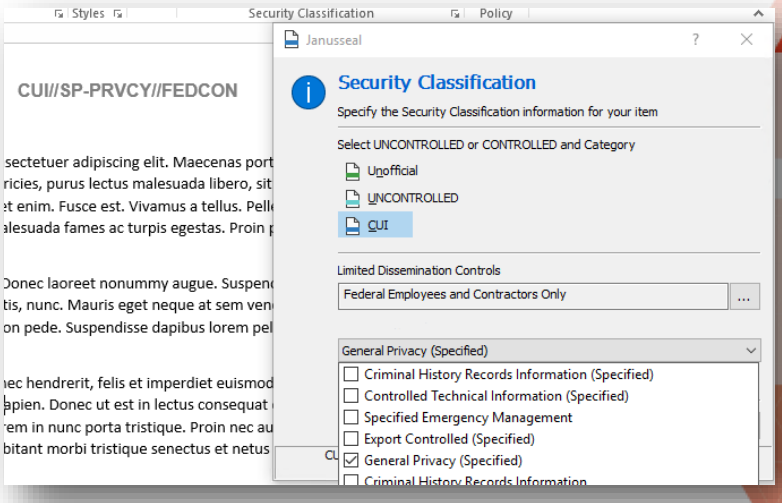
Across all sectors of the economy, there are increasing demands to access and use data in new ways, to help drive strategic decision-making. For-profit organizations want to extract greater value from the customer data they hold, while public sector agencies want data to yield insights to better inform policy-making and government service delivery.

Meanwhile the pandemic-led explosion in the growth of personnel 'working from home' has caused rapid-fire rollout of new technologies to enable data sharing across remote working environments.

However, there is a tension between opening up data for more users, new purposes or sharing via new technologies, and ensuring data is appropriately protected. Organizations need to manage information assets wisely to avoid data breaches, and must also juggle compliance with privacy and data protection laws.

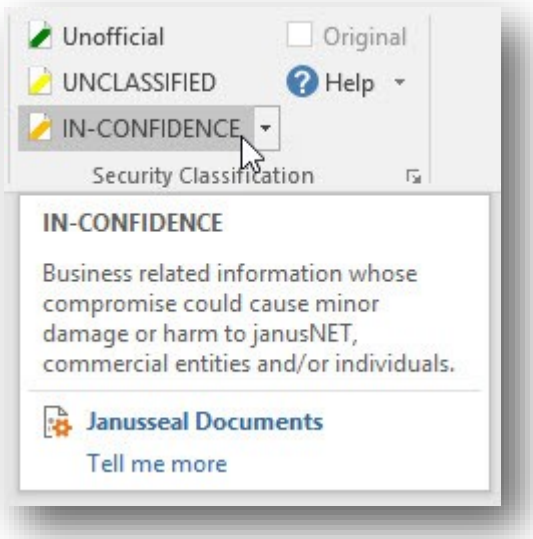
New privacy regulations focus on data security

Around the world, tough new laws have raised data protection to a matter of critical operational risk. While much compliance focus has been on the implementation of the 2018 General Data Protection Regulation (GDPR) in Europe since the GDPR's passage there have also been privacy law reform efforts in countries as diverse as Japan, Brazil, India, China, Australia and New Zealand, and in the State of California.



Janusnet

Data breach notification laws and more generalist privacy regulations have the objective of protecting individuals, thereby forcing companies and governments alike to implement more secure practices when handling data.



The GDPR, for example, requires organizations to notify any breaches of security leading to personal data being lost, or accessed, disclosed, modified, or destroyed without authority. In the first nine months after the GDPR commenced, more than 64,000 data breaches were notified to European data protection authorities, and more than €55M had been levied in fines.[1] By November 2019, 18 months after the GDPR's commencement, that figure had risen to more than 160,000 data breaches.[2]

Meanwhile, the California Consumer Privacy Act (CCPA) commenced in January 2020. This Act allows consumers to sue a business for damages from a data security breach caused by the company's failure to implement and maintain reasonable security procedures and practices to protect personal information. With compensation set at up to $750 per consumer per incident, or actual damages if greater, expect to see significant representative claims arise shortly.

However not yet even one year old, a new law was passed by referendum in late 2020 to further strengthen the CCPA. Amendments from the California Privacy Rights Act (CPRA) will come into effect in 2023 and will introduce significantly tougher requirements on certain categories of data, such as geolocation data. Given the extent to which geolocation data about customers is often casually collected via apps and shared with third parties to enable personalized targeting, the CPRA requirements will pose compliance challenges for organizations not able to identify and protect these categories of data.

Meanwhile New Zealand's reformed Privacy Act commenced in December 2020, introducing extra-territorial reach much like the GDPR and CCPA enjoy, and triggering data breach notification requirements. Australia's Privacy Act has had a mandatory data breach notification scheme since 2018, but a review of the legislation being conducted in 2021 is considering significant increases in penalties for non-compliance, as well as whether individuals should be allowed a direct right of action to sue for damages suffered from data breaches or other interferences with privacy[3].

[1] European Data Protection Board, *EDPB LIBE report on the implementation of GDPR*, 26 February 2019; available at https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf

[2] European Data Protection Board, *Contribution of the EDPB to the evaluation of the GDPR under Article 97*, 18 February 2020; available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf

[3] See https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988

Avoidable data breaches

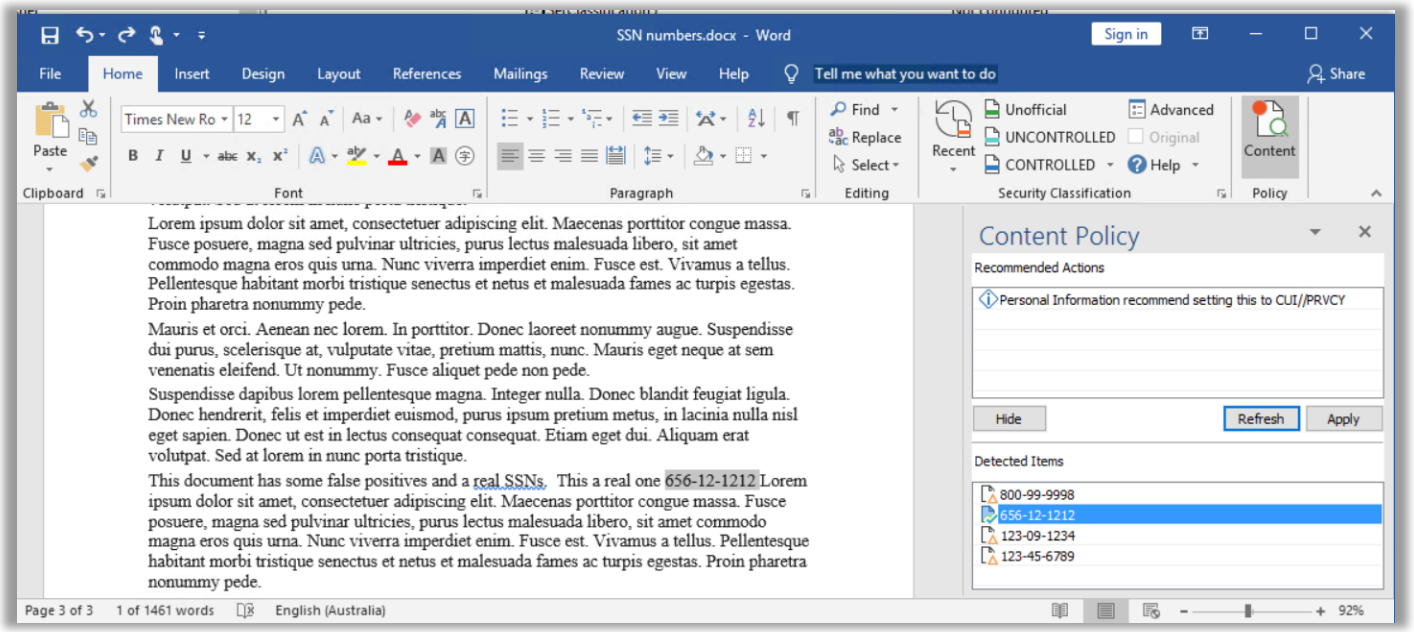
We now have a better understanding of the role of proper data handling in preventing data breaches. While detailed statistics from the European regulators are not yet available, evidence emerging from the Australian notifiable data breach scheme suggests a high degree of avoidable human error features in many data breaches.[4]

Of the notifiable data breaches reported in the first year of the scheme in Australia, 35 percent were the result of human error. Of those, the single most common cause of a data breach was personal information sent to the wrong recipient by email (29 percent). Failure to use BCC when sending an email accounted for another 7 percent of human error breaches.[5]

Thus more than a third of all data breaches caused by human error, or more than one in ten data breaches overall, involves sending emails. Emails are now recognized as raising the risk of unauthorized disclosure, with the Australian Privacy Commissioner for example expecting controls to be implemented to manage the transmission of personal information by email.

Another common but avoidable cause of data breaches is the failure to recognize that sensitive data even exists within a dataset to be shared or publicly released. Examples have included:

- Sensitive data embedded in a Word document published online
- Private phone numbers not redacted properly in published documents, and
- Credit card and passport numbers incorrectly entered in free-text fields, and not found before a customer dataset was shared widely.



[4] Under the Australian *Privacy Act 1988*, data breaches which are likely to result in serious harm must be notified to the Office of the Australian Information Commissioner (OAIC). The OAIC reports quarterly on the data breach notifications it receives; see OAIC Quarterly Statistics Reports at https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics-reports/

[5] Office of the Australian Information Commissioner, Notifiable Data Breaches Scheme 12-month Insights Report, May 2019; available at https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/

A final avoidable cause of data breaches is the 'workaround'. Secure data transfer protocols minimize the risk of data loss in everyday communications. Yet in the wake of the COVID-19 pandemic, many organizations shifted quickly to working from home arrangements, which can undermine standard methods for sharing data safely.

One example is the explosion in the use of online meeting and video conferencing platforms such as Microsoft Teams, Zoom, and Webex. Without additional tools to protect classified documents or sensitive information can be unwittingly shared in an insecure way, and data disclosed to unauthorized recipients. Simple things can make a huge difference to behavior. Visible markings make people think twice before sharing a document on a collaboration platform or transmitting it in email.

How Janusnet can help your organization share data safely

Corporations and governments alike must use a combination of governance, procedures, technologies, and systems to ensure that employees do not access information they are not supposed to and do not cause unauthorized disclosures of personal information, or other types of sensitive information such as trade secrets or 'classified' data. This is made easier with data classification because it distinguishes between sensitive and public information. Commonly this is done with visual markings in the headers and footers of documents, as well as in the first line of text (FLOT) in emails and subject lines.

Wherever possible metadata in the information object carries information about the security disposition, which makes it straightforward to program email gateways, access control systems to apply a corporate policy and prevent accidental disclosures.

Common causes of data breaches can therefore be avoided with Janusnet technology. In addition to the scenarios described above, Janusnet desktop and server products can be configured to prompt users to check if too many people are included in the To or CC rather than the BCC field, or if the proposed recipient of an email does not match the security classification of the contents of the email. Software can also be easy configured to block the transmission of sensitive material outside the organization's domain.

Janusnet technology can also be used to scan for sensitive content documents attached to an email, and then warn or block transmission depending on the recipient. The software can be configured to look for specific strings such as credit card numbers, passport numbers, social security, or tax file numbers, which should be redacted before sharing or public release. All this is facilitated with easy prompts to users, considerate of business workflows.

Contact us, or your Janusnet partner, to discuss how Janusnet technology can help ensure your organization is in a position to always share information safely.