TECHNOLOGY BRIEF

NCPROTECT™

GDPR COMPLIANCE FOR MICROSOFT SHAREPOINT DATA

The European Union General Data Protection (GDPR) is a law that is directly binding and applicable with heavy fines being imposed on those who are found to have not met the data protection requirements. Under GDPR, the EU's data protection authorities can impose fines of up to up to €20 million (roughly $20,372,000), or 4% of worldwide turnover for the preceding financial year – whichever is higher.

Top 10 GDPR Breaches

1. **Amazon**
   €746 million ($877 million)
2. **WhatsApp**
   €225 million ($255 million)
3. **Google Ireland**
   €90 million ($102 million)
4. **Facebook**
   €60 million ($68 million)
5. **Google LLC**
   €60 million ($68 million)
6. **Google**
   €50 million ($56.6 million)
7. **H&M**
   €35 million ($41 million)
8. **TIM**
   €27.8 million ($31.5 million)
9. **Enel Energia**
   €26.5 million ($29.3 million)
10. **British Airways**
    €22 million ($26 million)

EXECUTIVE SUMMARY

Since the introduction of the general data protection regulation (GDPR) in May 2018, organisations have been frantically developing plans to manage copious amounts of structured and unstructured data in a way that complies with both new and existing legislation.

SharePoint is one of the most widely used document management and data storage systems in the world, with thousands of companies using it to store essential business data ranging from intellectual property and operational data to documentation containing personally identifiable information (PII) about their customers, partners and employees.

Under the GDPR legislation, organisations are obliged to take inventory of the data they hold to ensure that personal or sensitive data is adequately protected to avoid significant financial and reputational damage in the case of non-compliance.

WHAT IS THE RISK UNDER GDPR?

As an organisation collecting and managing data, the personal data you collect is wholly your responsibility to protect. With SharePoint being utilised for a wide range of business activities, data can quickly be lost amongst vast amounts of other unstructured data. As organisations become more experienced in securing information residing in structured systems, malicious users refocus their efforts on unstructured data within systems with significantly weaker protection in place. It is this unstructured data that poses the highest risk, as bringing it under control to meet legislative requirements is far less trivial.

UNIDENTIFIED DATA

SharePoint has been in widespread use for well over a decade, which in many organisations means that content sprawl is prevalent. With new legal obligations to provide access to, rectify or remove personal data under the GDPR "Rights of the Data Subject" any of these documents containing a credit card number or passport could potentially cost the organisation millions in fines or reputational damage if not managed appropriately. If an organisation does not know what data their own employees have access to, they cannot effectively manage the liability that personal data presents under the new regulation.

NC Protect Data Discovery and Classification

With the ability to scan for and identify hundreds of data types, NC Protect can scan an entire SharePoint repository to reveal the information that must be protected under new legislation, enabling the Controller to perform their responsibility (GDPR Art. 24) of identifying, locating, minimising and protecting all personal data processing.

INSIDER THREATS

The exposure due to accidental, intentional or malicious sharing of documents containing personal data held by an organisation is not only high, but also very common. IBM's 2017 'Cost of Data Breach Study: Global Overview' reports 25% of all data breach incidents were internal, involving a negligent employee or contractor. To make matters worse, SharePoint users and administrators typically have access to far more data than they require to perform their roles.

NC Protect External Access Controls

By default, a SharePoint administrator has access to all data within the repository. Implementing fine grained access controls that are external to those of SharePoint plays an important role in eliminating single points of failure from a permissions perspective, and directly contributes to the "Data Protection by Design and Default" (Art. 25) and Security of processing" (Art. 32) requirements of the GDPR.

NC Protect implements granular attribute-based access controls (ABAC) that restrict individual file access to only to the right users or organizational groups. It ensures that administrators cannot access/view the sensitive information contained within a file or email.

DATA BREACHES AND REPORTING

GDPR requires organisations to report a data breach "without undue delay and, where feasible, not later than 72 hours after having become aware of it" to both the supervisory authorities and affected data subjects. Without GDPR endorsed security measures such as encryption or appropriate access controls, a SharePoint system can quickly become a huge liability with increased risks of damage to brand reputation, disruption of business operations, loss of revenue and threat of fines or penalties.

NC Protect Encryption

GDPR identifies encryption as a suitable means to safeguard personal data (Art. 32(1)(a)). By leveraging Azure RMS or proprietary AES-256 encryption capabilities, NC Protect can encrypt data at the file level to significantly reduce the impact of data stolen via breach or malicious user. A data breach will not need to be reported to the data subjects at all if their data is sufficiently protected by encryption (Art. 34(3)(a)) as the risk to the rights and freedoms of natural persons" is much lower.

INABILITY TO EXECUTE DATA POLICIES

GDPR demands that all relevant data sets are governed by policies for use and removal which is to be communicated to the data subject at the point of collection. Many organisations have little to no structure or policy to govern the way data enters SharePoint or how it is accessed, audited and removed. Communicating policies to a data subject may present a challenge, while implementing and enforcing these policies can be particularly difficult when dealing with various data types.

NC Protect Policies

NC Protect can perform a search using specific criteria to locate expired data so it can can be removed. Logging these activities provides sufficient proof to regulatory authorities that the Rights of the data subject" are being fulfilled. Simultaneously, it enables an automated, efficient process to execute the subjects right to access (Art. 15), right to rectify (Art. 16) and right to erasure (Art. 17). This equips an organisation with the tools to complete the required actions as a Processor where it's obligations are to aid the Controller in executing the request (Art. 28).

DISRUPTION TO BUSINESS OPERATIONS

Unprepared organisations will find themselves scrambling to adequately respond to a "Subject Access Request" when required under the GDPR. Similarly, organisations must provide "sufficient guarantees" and assurance to third parties such as partners, suppliers or customers, in their ability to adequately protect shared data. The inability to demonstrate such security or processing measures may have an impact on the business relationship, as this assertion is a core component to GDPR compliance. Performing exhaustive searches on unstructured data can lead to significant costs in man-hours for those without the appropriate tools in place.

NC Protect Discovery

In addition to initial discovery, NC Protect can perform on-demand searches for personal information relating to a particular individual in the case of a "Subject Access Request". By having NC Protect in place to respond with a documented and repeatable process, access requests can be actioned quickly and efficiently.

Data-centric Access Controls and Encryption

NC Protect's data-centric access controls and encryption combined with a comprehensive audit log of document access and actions provide an effective means to prove Processor adequacy to partners, suppliers or customers who require this assertion to engage in compliant data sharing or business activities under the GDPR.