White Paper

BUFFALO™

GENERAL DATA PROTECTION REGULATIONS

FOR IT ADMINISTRATORS, DECISION-MAKERS, AND OWNERS OF SMALL TO MEDIUM-SIZED BUSINESSES

Compliance for SMBs from a storage perspective

What is GDPR?

The **European Union's General Data Protection Regulation (GDPR)** intends to strengthen and unify data protection for all individuals within the European Union.

It also addresses the export of personal data outside the EU. Those organisations outside of the European Union but holding data on EU citizens are subject to GDPR.

Its primary aim is to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

GDPR contains mainly information about how personal data should be processed and defines the role of a processor and a controller of data. It also includes information on how to work with data protection by design and data privacy by default.

GDPR will come into effect on 25 May, 2018.

The implications of GDPR

Small and middle-sized businesses (SMBs) that hold data on EU citizens have responsibility for the protection of the data they store.

This data needs to be stored systematically and protected from theft and misuse.

SMBs also need to be able to meet GDPR data subject's rights which are as follows:

- **to be informed about data processing**
- **to access their data**
- **to rectify or delete their data**
- **to take their data to another organisation**

Data retention is also an important factor. Some types of data need to be deleted after a certain time has expired, for example personal data collected in connection to a product purchase and associated warranty.

In addition, there are other types of data that needs to be stored for a minimum amount of time, such as certain financial data.

In practise, this means that SMB's need to know where personal data is stored and be able to respond to data requests in a timely manner.

Those organisations that don't comply with GDPR run serious risks, in the event of a major systems breach, such as hackers stealing the contents of a customer database.

Financial penalties can reach an upper limit of €20 million or 4% of annual turnover, whichever is greater.

The need to comply with GDPR

Most large organisations are doing all they can to meet GDPR requirements. They are cognisant of the implications if their data is breached.

However some smaller and medium-sized organisations are adopting a ‘wait and see’ approach.

They believe that GDPR mainly addresses and affects big corporations that collect and deal with huge amounts of personal data, such as social networks, cloud providers or search engines.

Many of these organisations are waiting to see what happens when a peer company falls foul of the legislation.

This approach is potentially damaging given that the threat of insolvency or even closure as a result of GDPR penalties is very real.

GDPR applies to all companies; no matter how big they are or how much their turnover.

Data protection by ‘design and default’

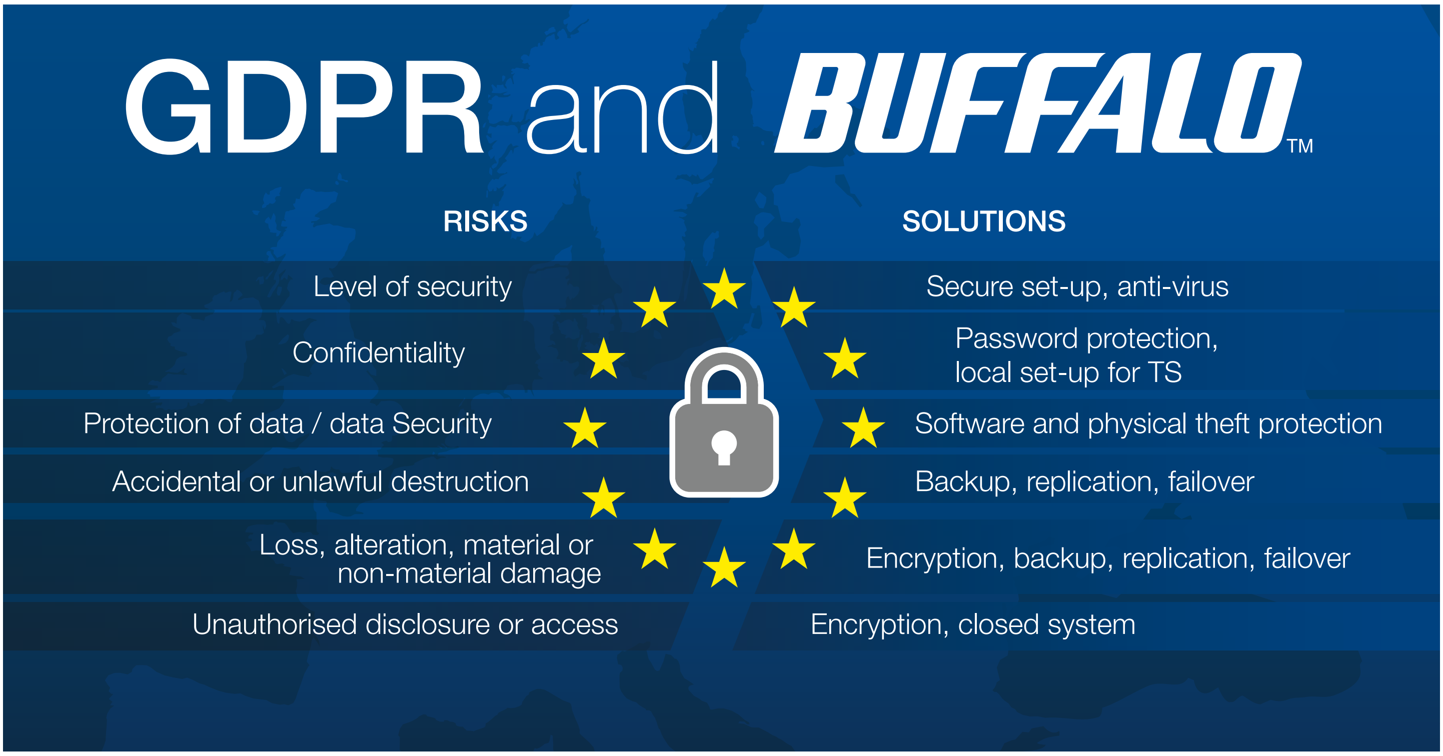
Under the GDPR mandate companies have to ensure they approach data protection by ‘design and default’.

At a high level it means that companies must secure their systems and processes to ensure data does not leak out or is easily hacked.

It requires that data protection is designed into the development of business processes for products and services.

This requires that privacy settings must be set at a high level by default, and that technical and procedural measures throughout the entire data processing lifecycle complies with the regulation.

Additionally, organisations need to implement mechanisms to ensure that personal data is only processed when necessary for each specific purpose.



GDPR and BUFFALO™

RISKS	SOLUTIONS
Level of security	Secure set-up, anti-virus
Confidentiality	Password protection, local set-up for TS
Protection of data / data Security	Software and physical theft protection
Accidental or unlawful destruction	Backup, replication, failover
Loss, alteration, material or non-material damage	Encryption, backup, replication, failover
Unauthorised disclosure or access	Encryption, closed system

GDPR data protection in practise

Data protection by design and default might directly impact your data storage solution.

The requirements mean you need data storage that is both easy to access and manage and also has privacy and protection designed into its foundation.

- If you plan to store data in-house, your business will be both the data controller and data processor. As a result it will be fully liable to the repercussions should any of this data be hacked or the regulations breached
- If you plan to use a public cloud or hybrid-storage solution, it is the responsibility of the business to ensure that it and the third-party provider are GDPR compliant

If personal data is stored in-house on a server, network attached storage (NAS) or other devices, to ensure GDPR compliance the following features should be incorporated into the storage device:

- **Password protection –** Devices and files and / or folders that contain personal data should be protected by passwords. They should only be accessible to users who have the permission to access and / or process the data
- **Encryption –** data should always be encrypted whether stored or transferred
- **Physical protection from theft / loss –** devices that store personal data should have physical protection such as a Kensington lock or keys for NAS and hard drives in a server, or similar
- **Anti-virus software** to ensure that data isn't infected with malware such as ransomware
- **Firewall protection**
- **Backup and Restore –** backups should be automated and carried out daily so in the event of data loss the most recent copies of personal data can be retrieved

Furthermore there are several other additional measures that are equally important:

- A storage device that provides RAID redundancy and protects against hard drive failures avoids system downtime and data loss
- Centralised storage should be preferred over local storage on PCs, laptops or external or portable hard drives. These devices are more prone to theft and unauthorised access. It's also extremely difficult to control who has access to them and the data on them

Closed System

Secure Set-up

Data Encryption

Passwords

Anti-Virus
(TS3000/3010 & TS5000/5010, sold separately)

Backup, replication, failover and encryption

Anti-Theft Features
- Software Protection: Boot Authentication
- Physical Theft-Protection

GDPR fundamentals for SMBs

There are some fundamental storage security steps that SMBs need to take to ensure they meet GDPR mandates for protecting personal data.

Storage root directory

The root directory is like the main trunk of a tree from which all the other branches spring out of. If a hacker gains access to a root directory they can hide viruses and malware in plain sight by disguising malicious code as important files which antivirus software will overlook.

As such NAS operating systems need to be closed so even the system administrator can't gain access. This firmly shuts down loopholes that are exploited by hackers who commonly use sophisticated rootkit tools to access root directories.

Secure setup

Often when a company is configuring a NAS system an internet connection is required to set up the account and enable remote access. For some NAS systems this is standard practice.

However, it is also a process that hackers exploit, stealing usernames and passwords as data travels outside of the company network and across the internet.

Strong encryption

Data that is stored on hard drives can be stolen. Encrypting the hard drive with 256 AES encryption, which is theoretically unbreakable, means the data cannot be read even when the drives are removed.

Buffalo TeraStation™, the securest NAS and fully GDPR compliant

Buffalo TeraStation™ NAS, specifically designed for SMBs, provides the following features, all of which ensure full GDPR compliance.

- There is no back door access which means hackers can't access the data storage through common methods such as SSH protocols or Telnet servers. In short, data cannot be hacked nor can it be destroyed.
- There is no function or options in the TeraStation™ firmware operating system to change or add features. Essentially, it is locked down and as a result, the potential for unwittingly creating security vulnerabilities that could be exploited by hackers are negated.
- A software option allows a user to prioritise data security over system access by disabling external restores / resets.
- TeraStations™ are physically protected by cable locks and lockable hard drives. These physical restraints protect the hardware from actual theft while boot authentication in the software denies access to the data under any circumstance.
- Includes AES hardware encryption for hard disc drives. This is not turned on by default but can be easily activated. It essentially locks down the hard drive so should somebody remove the drives data can't be accessed.
- Incorporates secure file sharing protocols (HTTPS, SFTP) for secure local and remote access. Data is never sent as clear text over the internet so it cannot be read by third parties or hackers.
- To improve the performance, reliability and security of data storage secure RAID modes are preconfigured at the factory.
- Each TeraStation™ includes HotSwap 24 hour hard disc drive replacement to ensure the storage is always intact.
- TeraStation™ firmware cannot be infected with viruses because it is a closed system. That said files and shared files used between computers, tablets and smartphones are always at risk of malware infection, such as ransomware, spyware and Trojans when these devices connect to the storage. The antivirus option, updated frequently with the latest virus signatures and designed to detect zero day threats, keeps all files free of malware.
- Multiple backup options are available to safely store files on or off the NAS. The options include regular backups, data replication, failover, cloud backup, USB or NAS backup and PC and server backup

There are several Buffalo TeraStation™ models available, each one designed to meet the specific needs of different sized organisations.

The gatekeeper

Central to successful GDPR compliance for SMBs is the need for a company gatekeeper who takes responsibility for managing and protecting customer data.

Nominating an 'individual' as compliance gatekeeper ensures a consistent focus.

The gatekeeper can identify compliance gaps, map out needs and introduce and monitor management processes that dovetail with requirements.

In short, they become the GDPR compliance 'expert' and the fulcrum for successful compliance.

GDPR definitions

GDPR refers to data controllers, data processors and data subjects.

- Data controllers are organisations that collect data from EU residents, for instance, an online or offline business that trades in the EU and holds personal customer information such as names, addresses, payment information.
- Data processors are organisations that process data behalf of the data controller such as a cloud service provider.
- Data subject is an EU citizen or resident whose information is held by a data collector or processed by a data processor.

Many SMBs will likely be both data controllers and data processors.

GDPR definition of personal data

Personal data is defined as any information related to a EU citizen that can be used to directly or indirectly identify the person.

This can include anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information and even a computer IP address.