NetApp and the General Data Protection Regulation (GDPR)

A comprehensive guide to help prepare NetApp's customers for the May 2018 GDPR deadline

June 2017

NetApp

TABLE OF CONTENTS

1 Introduction - NetApp and Data Privacy

As the world's largest independent enterprise data management vendor, and leading expert in data for 25 years, NetApp understands the complexity of data privacy laws, including GDPR and the steps it takes to build a globally recognised, compliant program. We are now helping customers on their own journey towards compliance. This is drawn from our model of excellence and our experience of enforcing stringent data privacy and data protection processes in our business, as part of an extensive data governance strategy. This strategy allows us to respect the fundamental right to privacy of our employees and customers while maximising the potential of our data, and yet maintain compliance. .

2 GDPR: Understanding data privacy compliance and the business implications

The General Data Protection Regulation (GDPR) is the biggest overhaul of EU data protection law in over twenty years. It will replace the current EU Data Protection Directive and aims to create a unified data protection legislation covering all individuals in the European Union. It was adopted by the European Commission in April 2016 and will come into force on 25th May 2018.

GDPR is a dramatic change to the way the collection, access, use, storage and transfer of personal data is regulated. It will affect any business which has access to or processes the personal data of an EU resident, regardless of where the business is located. The extraterritorial nature of the regulation will be felt globally. Under GDPR, the rights of individuals to own and control their own data are strengthened, and key tenets of the legislation include:

1. The right to transparency
2. The right to provide explicit, unambiguous, freely-given consent
3. The right to restrict processing
4. The right to object
5. The right of access
6. The right to restrict automated decision making and profiling
7. The right to rectification
8. The right to erasure
9. The right to data portability
10. Greater obligations and accountability on data processors

GDPR is first and foremost a legal compliance issue, achieved through a robust data privacy compliance framework. Understanding privacy laws along with transparent policies, procedures, processes, consents, and notifications are the foundation for achieving GDPR compliance. This legal foundation must be in place before investing in tools and technology. The introduction of tools and technology are a later step in the compliance journey and will allow companies to maintain (not obtain) ongoing compliance with the regulation.

2.1 Why is GDPR important?

Undeniably, data is crucial for modern business. With media decrying data as the ‘new gold’ and the exponential growth in personal data available to businesses, GDPR is set to re-focus the business agenda on data privacy – thus reaffirming consumer trust. The legislation will make it essential for all businesses handling the personal data of EU citizens to understand exactly where their data is stored, ultimately taking responsibility for the data it processes. The implications of failing to comply are significant : fines of up to 4 percent of global annual turnover, or up to €20m – whichever is greater.

One important distinction to make in achieving GDPR compliance is between data privacy, data security and data protection. Security is not privacy. Data privacy is the full lifecycle of the personal data from the time you collect it to the time you destroy it. A useful analogy is to think of a filing cabinet – privacy is the contents in the cabinet, the cabinet lock is the security, and making sure that only the right people have access to the content is the protection. While data security is certainly important for businesses, encryption and data masking will not help a business become GDPR compliant. It doesn’t help companies if they secure data they are not legally allowed to have. The process towards achieving compliance needs to be led from the C-suite down, as a legal and business concern before a technology one.

2.2 Why should businesses care about GDPR?

Companies need to understand GDPR is a legal obligation, but they also need to understand it can become a key business differentiator. In short, companies that are fully compliant are likely to be viewed more favourably in the market compared to those that are not compliant. When a customer is deciding whether to work with a company, they will increasingly defer to the business that can clearly prove they understand data privacy, and have an effective data governance strategy in place – at its fundamental level, it is proof of responsible business practices.

At the same time, the process of becoming compliant with GDPR requires businesses to get to grips with exactly what data they have, whether they have the right to have it, where it is stored, what they’re allowed to do with it and who has access to it. With this knowledge, businesses are in pole position to make better business decisions, effectively utilising the data resources at their disposal.

2.3 How can businesses achieve GDPR compliance?

While the process of achieving GDPR compliance is complex, a brief overview of the steps businesses need to take is as follows:

1. Make sure you understand the requirements laid out in the GDPR, and seek appropriate legal advice where required.
2. Understand what data you have that could be classed as the “personal data” of any EU citizen – this can include images as well as traditional text-based data – as well as where it is stored.
3. Ensure you obtain the explicit, unambiguous and freely-given consent of each data subject.
4. Minimise the personal data being collected – as businesses now need to be transparent on what data they’re collecting and why, ensure that the personal data you are collecting is a “must have” for your business, and not just a “nice to have”.

5. Make sure you are able to easily access personal data in order to fulfil "Subject Access Requests" or "Right to be Forgotten" requests.
6. Make sure you have transparent and easily understandable policies and processes in place so there is no ambiguity about what data you are collecting and what you are doing with that data.
7. Make sure you have a clearly documented and tested Incident Response Plan and team to meet the 72-hour data breach notification requirement.

This process requires getting to grips with the GDPR and how it relates to each specific business, which will take a significant time investment. However, once a company builds the legal compliance framework and their policies and procedures are in place – as well as their understanding of what data they have, why they need it and where it is – they will be in a stronger place to make informed technology decisions, to ensure that they can maintain their new level of compliance.

While achieving GDPR compliance is certainly a process and does take time, it can also provide a crucial opportunity for a "spring clean" of your data. By making sure you know which data you need (the "must have" data), and then getting rid of unstructured and excessive legacy backups (which may be "nice to have", but are often difficult to navigate or use effectively), businesses can efficiently maximise their storage resources and ensure better data management both now and in the future.

3 Why NetApp is a leading authority on GDPR:

Having prioritised compliance with data protection laws, NetApp has earned the highly distinguished Binding Corporate Rules (BCRs) approval – EU recognition of a set of stringent, intra-corporate policies that allow multi-national organisations to prove personal data across borders is compliant with EU data protection laws. This validates its commitment to the fundamental rights of all individuals to the right to privacy. Acknowledging the growth of globalisation and consolidating our position as an industry leader in data privacy, NetApp chose to go beyond the US centric Safe Harbor data legislation (which is now defunct as an adequate data protection framework) or its Privacy Shield replacement, instead embracing the laws of every country in which it operates.

NetApp is also required to justify its use of third parties with access to collected personal data. While achieving BCR status may be a long and arduous process, it reinforces NetApp's commitment to data privacy by shoring up compliance vulnerabilities to a robust standard that will withstand the highest level of scrutiny – it is now more than 95 percent compliant.

Leading by example, NetApp has embraced its responsibility to protect personal data from unauthorised collection – it is one of less than 100 companies worldwide using BCRs – placing it at the forefront of data protection, as the leading authority on GDPR. Embracing our role as a thought leader, NetApp created the Cloud Survey, seeking to understand the level of awareness and preparedness of EMEA businesses ahead of the GDPR deadline. While 73 percent of base respondents say they have some concerns about meeting the deadline, almost a tenth (9 percent) still do not know what GDPR is, suggesting we have some way to go in terms of educating businesses on the implications of the upcoming legislation.

NetApp's exemplary consultancy led approach, with a focus on educating businesses on GDPR, sets it apart from its competitors – many of which lead with a 'technology first' approach. HPE's recently launched GDPR toolkit provides a case in point, focusing on software solutions without first addressing the worrying gap in understanding and awareness of GDPR among businesses. This is like sticking a plaster over a wound with your eyes closed – it is essential that businesses understand the complex nuances of the GDPR in order to carry out a thorough assessment of their data management, before sourcing a solution.

NetApp's GDPR solution:

- *GDPR legal and compliance consulting*
- *E-discovery*
- *Case management*
- *Solution mapping for compliance maintenance*

3.1 Achieving GDPR compliance with NetApp

As an exemplar in data privacy, NetApp can help businesses prepare for GDPR, thanks to its team of data privacy experts and its holistic solutions. As preparation for GDPR requires a compliance process led solution, we strive to educate customers first on the foundations of data privacy compliance and secondly on technology solutions. By factoring in people, processes and finally technology mapping across the ecosystem, NetApp promises robust support for businesses seeking GDPR compliance.

The first step towards creating a holistic solution to meeting GDPR is seeking expert advice from qualified consultants. In our view, it is essential that we help the client first understand their current level of privacy, identifying the gaps between what is required by GDPR and the current provision for data privacy – and the risks and vulnerabilities these pose. In order to minimise and address these risks, we then define the antidote and implement the appropriate level of governance within the project and across the entire business environment. Ultimately, data privacy should be at the fore of any business decision. A fundamental part of our consultancy is to educate businesses on the compliance responsibilities within GDPR, before recommending solutions.

Once businesses have received the expert advice required to make the necessary changes, it is time to look to the ecosystem. This means running assessments of the following criteria:

- **Data Discovery –** understanding where and what your data is stored on.
- **Unstructured data analysis –** understanding your unstructured data in files, home directories and shared drives, for example.
- **Backup data analysis –** backups in backup vendor formats.
- **Cloud data analysis –** the unstructured data held in the cloud, for example in OneDrive.
- **Structured data analysis –** identifying structured data hosted in databases, data warehouses, Business Intelligence and mainframe applications.
- **Data lineage –** capturing the lifecycle of your data, from capturing to transformation and use.
- **Data case management –** for uses such as Legal Search and Hold, the right to be forgotten and coordinating a case request.

One key component of the ecosystem to highlight as part of a GDPR compliant program, is data lineage. This element essentially requires understanding a business' data journey from initial capture, through to transformation and data use. NetApp's data lineage partner solutions involve mapping data's lifecycle across a heterogeneous technology environment and providing a clear oversight to business policies and regulations.

Another key component in NetApp's holistic approach is case management. Using eDiscovery (the process of obtaining electronic data with the intention to use it as evidence in a legal case), data case management and data governance partners, NetApp's solution protects file and email servers from cyberattacks and insider threats. The data security platform analyses the behaviour of the people and machines that access data, so that businesses can identify compromised accounts, privilege escalations, Group Policy objects (GPO) changes, and malware attacks like ransomware – and stop them before they lead to a data breach.

Once compliance processes have been established across the business ecosystem, mapping the appropriate technologies to help maintain ongoing compliance is essential. Our unique data management capabilities found throughout our Data Fabric portfolio – a unique data management software portfolio ensuring the right data can be found in the right place, at the right time, by the business applications that need access to that data – enable businesses to easily access data, improve visibility, security and portability of data. Each article of the legislation can be meticulously reinforced with NetApp and partner technologies. In order to maintain compliance beyond the May, 2018 deadline, this final element will be crucial.

4 Why choose a NetApp solution?

Placed at the forefront of the landmark changes in data governance, NetApp's expert consultancy on GDPR stands to educate businesses on the processes required to meet compliancy by the May, 2018 deadline. Leading by example with its robust data privacy processes in compliance and adhering to arguably the most stringent global data privacy standards with its BCRs, NetApp sits in an elite top 100 for data privacy and compliance.

Our solutions ensure all angles of business are covered throughout the ecosystem, meeting all the complex needs of GDPR, while enabling businesses to better manage their data through the lens of data privacy by design. By combining a consultancy led approach, with a focus on the mapping of supporting technologies NetApp is positioned to set businesses up for a world that is increasingly driven by data.

As the Internet of Things (IoT) takes off, with 80 billion connected devices expected by 2025 according to IDC, legislation will need to evolve in tandem with the surge in data. Businesses can no longer hide from the privacy issue. They must act now or risk future business fines and potential reputational damage, if a breach occurs. Enlisting NetApp's portfolio of Data Fabric solutions will put customers at the forefront of the data management processes – and at the heart of compliance.

GDPR Articles & how Technology can help	NetApp’s Technology Approaches & Solutions
Article 6: Processing not Allowing Identification How technology can assist in maintaining Article 6 • Anonymization (or pseudo-anonymization) of data would enable subject data to be processed within the terms of the GDPR. Data that is not traceable back to an individual may be processed. • From a technology perspective, technology can provide both the means to anonymize data, to automate the process of anonymization and to audit the process wrap around this.	**NetApp technology helping maintain GDPR compliance** • NetApp’s **SnapManager/SnapCenter** tools enable databases to be cloned, for alternate purposes such as data mining, processing etc. **SnapManager** can incorporate a 3rd-party masking technology that could be used to provide the necessary data anonymization required by the GDPR. • Automation of any process, anonymization included, reduces errors, implements standardization and speeds operation. NetApp’s **WorkFlow Automation** tool is ideal for automating data management and anonymization processes. **OnCommand API Services** provides centralized integrated monitoring of storage infrastructure.
Article 17: Right to Erasure and To Be Forgotten How technology might maintain meeting requirements for Article 17: • Article 17 looks at the data that is held by an organization and the right of an individual to erasure and removal of that data. This does not necessarily apply though if there are overruling laws or regulation. • To be able to erase data, you need to understand where that data is. You need to understand where physical copies are paper/files/backups/archives etc., you need to understand the linkage/lineage of how that data connects through your organization and you need to ensure that you have sufficient mechanisms in place to allow for timely action of an erasure or Right to be Forgotten request. • Technology can apply physical and logical data discovery tools, can enable data linkage lineage to be established and maintained and can accelerate the process or discovery, linkage and potential erasure.	**NetApp technology helping maintain GDPR compliance** • **OnCommand Insight** enables a physical view of infrastructure and can help identify the primary and secondary copies of data, both on-premises and in the cloud. Logical discovery of data can be identified through partner tools from companies such as **Varonis**, Veritas and Commvault, to name but a few. • Unstructured data is difficult to track, but technologies such as **StorageGRID Webscale,** enable an organization to store unstructured data in a more organized fashion. Object data can be assigned metadata and then dynamically managed with policies, even where that data spans hybrid clouds. • With **WorkFlow Automation**, decisions to delete or manage data can be automated for speed and accuracy. **Service Level Manager** simplifies storage service delivery, and optimizes storage operations for predictable, consistent service.

Article 20: Data Portability How technology might maintain meeting requirements for Article 20: - Article 20 concerns the right of the data subject to receive their data in a format that is structured and commonly digestible. That data should also be available for transmission to another data controller, for example when changing service providers. - Technology will be involved in the translation of data into a structured common machine readable form, but also in enabling the transportation of data from one data controller to another, even where this may involve differing source and destination systems.	**NetApp technology helping maintain GDPR compliance** - As with data transfer, the capability of NetApp's **Data Fabric** allows organizations to deploy multiple remote end points either on-premise, in the cloud or at a 3rd party location. - **SnapMirror** can act as the underlying transport mechanism for transmitting that data from location to location in an efficient and controlled fashion.
Article 23: Data Protection by Design and Default How technology might maintain meeting Article 23: - Article 23 directs that data protection should be considered in any product by design and by default. - You cannot embed privacy in technology products, but you can incorporate and build features that will enhance privacy. - Consider the use of technologies that restrict access, implement role-based access and encryption. - Data Privacy also supports the right of access by the data subject, to that data. Technology can support this by ensuring the data is highly available, protected, recoverable and maintains integrity. - Data Privacy also supports the right of access by the data subject, to that data. Technology can support this by ensuring the data is highly available, protected, recoverable and maintains integrity.	**NetApp technology helping maintain GDPR compliance** - Whilst NetApp does not provide explicit products that will provide customers with privacy, we do design and build products that allow our customers to comply with data privacy laws, especially GDPR. - From NetApp's perspective consider our products that provide: – Encryption (Self Encrypting Disks, NVE) – Data Access Controls (RBAC, LDAP integration etc) – Data Integrity, availability & performance (HA, Business Continuity, RAID, DR, Flash) – Data Recoverability (**SnapShots**, S**napRestore**, **FlexClone, AltaVault** etc.) – Data Transportation (**Data Fabric**, **SnapMirror**, **S3**).

Article 25: Privacy by Design How technology can assist in maintaining Article 25: • To ensure only the minimum data is collected, processed and retained, by deleting from all sources as required and ensuring classification.	**NetApp technology helping maintain GDPR compliance** • Metadata and Policy controls for data – **StorageGRID Webscale** enables an organization to create a data lake, where metadata is used to track the profile and policies of unstructured data stored. Examples: whether data stored contains private information. How long data is required for processing and retention, sovereignty restrictions, application use. Consent status etc. • Encryption is available across NetApp's portfolio and enables organizations to secure their data from theft or loss. Partner technologies from companies such as **Gemalto** can further secure data. • High availability is a feature of NetApp's primary data management systems, and essential for delivering always available data.**StorageGRID Webscale:** enables an organisation to create a data lake, where metadata is used to track the profile and policies of unstructured data stored.
Article 30: Records of Processing Activities How technology might maintain meeting Article 30: • Article 30 requires that records are maintained around the processing activities of data, who controls access, data transfers, time limits for deletion and the security and data protection measures implemented. • Technology can assist in the recording of records, the discovery and classification of sensitive files and maintaining metadata about who can access, control of access and when data should be deleted. For unstructured data in particular, the application of object technology with metadata tracking and dynamic policy action could be key. Immutable records recording could also be used to prove a chain of authenticity and tamper-free recording.	**NetApp technology helping maintain GDPR compliance** • Without records of compliance for GDPR, the potential for larger fines is very real. NetApp provide highly available, disaster recovery protected data management platforms to ensure your compliance records are always available and protected • Add **SnapLock** for immutable records storage, proving those records have not been modified, tampered or accidentally deleted.

Article 32: Security of Processing How technology might maintain meeting Article 32: • Article 32 touches on the security of processing; asking pseudo-anonymization and encryption are used, as well as ensuring that systems processing subject data maintain integrity, availability and resilience. Article 32 also requests that restore procedures are available, and that access to data can be delivered in a timely manner. Apart from delivering these requirements, Article 32 also states that this must be tested regularly. • Technology can deliver: encryption, anonymization, reliability, availability, recoverability, performance and non-disruptive testing. Immutability could also enhance the recording of activities and auditing.	**NetApp technology helping maintain GDPR compliance** • Encryption is available on all of NetApp's portfolio, ensuring secure storage of data. • Performance, Integrity, Availability and Resilience are core features of NetApp's primary data management platforms, **ONTAP, SolidFire & E-Series**. • The ability to restore data, through the use of **SnapShots**, from primary, DR or cloud locations is a key differentiator of NetApp's **Data Fabric**. Protect subject data from **Ransomware**. • **StorageGRID Webscale**, enables unstructured data to be stored in a more organized fashion. **AltaVault** provides backup and archive to the Cloud. • Non-disruptive **testing** through the use of **FlexClone** enables an organization to regularly test data accessibility and security • Prove data has not been tampered or modified with **SnapLock.**
Article 35: Data Protection Impact Assessments (DPIA) How technology might maintain meeting Article 35: • Article 35 is concerned with ensuring that when data is processed and is considered high risk or sensitive to individuals, it is properly assessed to ensure appropriate data protection is applied. • Article 35 requires that an organization knows where its data is, not just the primary copy, but secondary copies too, on-premise, service provider and cloud. With knowledge of where data may be located, Article 35 requires that a DPIA is performed on high-risk and sensitive subject related data and that note is made of the reasons, use and data protection applied to that data. The DPIA records must be maintained as new systems (and processing) are added and the records must be available for access.	**NetApp technology helping maintain GDPR compliance** • **OnCommand Insight (OCI)** – Understanding what data requires a DPIA requires that an organization understands where its data is. OCI enables an organization to identify what virtual machines, servers and arrays that may be within scope to assess. With the ability to tag applications a company can define the scope of a data discovery exercise and the subsequent governance that should be applied. Without OCI, a company may understand its logical data view through its structured systems, but fail to fully identify data located outside of those systems. The **OCI Data Warehouse** can be used to link infrastructure discovery to data governance applications, such that new data repositories are actively identified and reported on. • DPIA records are fundamental to avoiding or reducing potential regulatory fines. **SnapLock** could be used to enhance the security and immutability of those records

Article 44-50: Data Transfers	**NetApp technology helping maintain GDPR compliance**
How technology might maintain meeting Articles 44-50: • Articles 44-50 place restrictions on the transfer of data between organizations and across international boundaries. Having in place Binding Corporate Rules (BCRs) is one of the criteria for making this permissible and NetApp globally already have these in place. • Technology is a fundamental part of a data transfer process, and the ability to create commonality of technology end-points enables data to be transferred more cost effectively, easily and efficiently.	• The **Data Fabric** connects the myriad of end-points that we can provide. This enables organizations to transfer data between data centres, remote offices, cloud locations and 3rd parties, all through the capabilities provided by **SnapMirror** and the **Data Fabric**.

5 Glossary

Binding Corporate Rules (BCRs) – A set of rules designed to help multinational organisations to transfer personal data from the EU across international boundaries within the organisation.

Case management solutions – In relation to GDPR, case management solutions are technologies that manage and track an individual's request for the right to be forgotten.

Data Governance – Data governance is the management of data, covering strategy, processes, accountability, usability and security.

Data Discovery – Data discovery solutions help businesses understand where their data is, what personal information it contains, and also ensures that the information can be found on demand.

Data Lineage – Data lineage is a data's lifecycle, incorporating its origins and movements throughout this time.

Data Privacy – Data privacy is the legal right to collect, process, access, host, store, share, transfer and/or destroy personal data. It is the laws and regulations that mandate the fundamental right to privacy in respect to an individual's personal data.

Data Protection – Data protection is the process of safeguarding data from corruption or loss, and includes backup and recovery of data.

Data Security – Data security is the technical fortress around data to protect against unauthorised access or use.

E-discovery – The process by which electronic data is found, secured and searched.

Personal data – Within the GDPR, personal data means "any information relating to an identified or identifiable natural person" either directly or indirectly, in particular including any forms of identifier, location data, IP addresses, or references to the "physical, physiological, genetic, mental, economic, cultural or social identity of that person."

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NetApp®