NetApp, Inc. (NetApp)
Data Protection
Binding Corporate Rules (BCRs)

Effective 081215
NetApp BCR vs. 9.0

TABLE OF CONTENTS

Error! Bookmark not defined.

1 INTRODUCTION

This document has been developed by the Worldwide Legal Operations, Data Governance function in order to define NetApp's policy and standards in regards to the protection of all personal and/or sensitive data collected, processed, used, stored, shared, and/or transferred anywhere in the company and/or to external third parties. These Binding Corporate Rules (BCRS) are binding for all NetApp Group companies. Once approved by the Dutch DPA and the co-reviewers of the BCRs (Spanish and Bavarian DPAs), as well as all other applicable Data Protection Authorities, the Rules will be communicated to all NetApp employees and contingent workers on our internal legal website and through an internal employee communication email and published on the external NetApp website at www.netapp.com

1.1 Introduction to BCRs

NetApp's Binding Corporate Rules (BCRs) define our approach to, and framework for, compliance with all relevant data protection laws, including the transfer of data outside of the country of origination. NetApp strongly supports the fundamental rights to privacy and data protection, as well as compliance by all our business entities with national and international privacy laws. We believe that appropriate privacy protection is a business enabler, not a barrier. Privacy protection can be a means to develop employee and customer confidence and trust, and develop lasting and positive employment and business relationships.

All NetApp companies, employees, contingent workers, customers, suppliers, partners and any other individuals must comply with these BCRs in connection with the collection, processing, storing, sharing and/or transferring of any personal data. Additional privacy regulations may apply to specific business functions such as Human Resources, Finance, Marketing and Sales. All members of the NetApp Group of Companies are obligated to respect and comply with these BCRs

The BCRs apply to all personal data of NetApp employees, customers, clients, suppliers, partners, prospects, and any other data subjects whose personal data is collected and used by NetApp. These BCRs will be posted on both our internal and external websites.

These BCRs also include our practice of implementing standard contractual clauses and transfer agreements both internally and externally to ensure that all relevant data protection laws are met when transferring personal data outside of the country of origination and/or outside the European Economic Area (EEA). NetApp requires any data transfers be governed by data privacy transfer agreements, clearly stating the responsibility of the data controller/data exporter and the data processor/data importer.

1.2 What are BCRs?

In regards to data protection, BCRs are an essential tool to protect the privacy of a data subject's personal data while facilitating international global transfers of personal data to corporate groups in countries without sufficient data protection legislation. BCRs allow companies to transfer personal data around the world using a single set of rules. This gives data subjects the confidence that their personal data is being processed using a

binding and enforceable set of standards. BCRs can also simplify the approval of data transfer mechanisms by DPAs. BCRs can facilitate data flows for companies, reduce their uncertainty about compliance, reduce administrative burdens on DPAs and increase the confidence of data subjects.

1.3 Binding Nature of BCRs

NetApp BCRS are made binding upon all members based on unilateral declarations or undertakings made or given by the NetApp's parent company, which are binding on the other member of the Group.

These Binding Corporate Rules (BCRS) are binding for all NetApp Group companies. All NetApp companies, employees, contingent workers, customers, clients, partner and suppliers have a clear duty to comply with and respect our BCRs. Internally, within NetApp and its companies, the rules are made binding through the implementation of

- The Rules
- Unilateral declarations by the Board that binds all NetApp group companies
- Intra-group model contracts/transfer agreements
- Data privacy-specific Non-Disclosure Agreements (NDAs)
- Internal regulatory measures
- Global data privacy policies

Employees are bound by the BCRs through:

- The Rules
- Individual model contracts/transfer agreements
- Data privacy specific Non-Disclosure Agreements (NDAs)
- Works Council Agreements
- Employee Code of Conduct with sanctions
- Internal policies with sanctions

Third party providers are bound by the BCRs through:

- The Rules
- Contractual obligations with sanctions
- Model contracts/transfer agreements
- Data privacy-specific Non-Disclosure Agreements (NDAs)

1.4 Contact Information

Any questions regarding these BCRs, your rights under the BCRs or any other privacy related questions can be directed to NetApp's Worldwide Data Governance Office at the following addresses:

Privacy@netapp.com

NetApp, Inc.

Worldwide Legal Operations

Attn: Ms. Sheila M. FitzPatrick

Chief Privacy Officer

495 E. Java Drive

Sunnyvale, CA 94089, USA

1.5 What are Privacy Laws?

Data Privacy Laws (also known as Data Protection Laws) were enacted to protect the personal data of all data subjects from unauthorized access and use. The laws give data subjects the right to control how their personal data is used, who can access it, and when and if it can be shared with a third party. The laws also define how organizations must manage and protect the personal data, as well as the restrictions regarding the transfer of any personal data outside of the country of origination or the EEA.

1.6 How Do Privacy Laws Impact NetApp Globally?

NetApp, Inc. and its subsidiaries transfer personal data internally, and to approved NetApp partners, for a variety of legitimate reasons connected to the functional, technical and operational requirements of the global business.

For instance, personal employee data may be transferred for the administration of employee payroll, benefits, stock program, internal education and development programs, finance activities (e.g. expense processing, corporate credit card management) or the corporate travel program. Customer personal data may be transferred in order to provide product support, technical services, warranty and maintenance renewals, product upgrades, and relevant events of interest to our customers. Prospect information may be collected and transferred for the purpose of providing relevant information regarding NetApp products, services and events to interested parties.

All transfers of personal data are done with the highest levels of security available and, when required by law, with the explicit consent of the data subjects.

1.7 How Does NetApp Address Compliance with Privacy Laws?

Adherence to data privacy laws and the respect for privacy are fundamental to NetApp's culture and help us maintain an environment where data subjects can trust us and our technology, and feel safe that their data is protected from unauthorized access, use or loss. Our BCRs are designed to provide a high level of protection for all personal data collected and processed by NetApp or by a carefully screened partner on behalf of NetApp. The BCRs apply in all cases where NetApp collects, processes, uses, stores, shares, and/or transfers personal data, whether online or offline, or by manual or automatic means.

The BCRs apply globally and ensure that NetApp's collection and processing of personal data complies with all country-specific data privacy laws, especially the European legal requirements. The BCRs are available on NetApp's internal intranet and external website and can also be obtained by requesting a copy at privacy@netapp.com.

1.8 Responsibility for Compliance

NetApp's Global Chief Privacy Officer (GCPO) is responsible for overseeing and ensuring compliance with the BCRs and establishing the global framework for data privacy compliance. The GCPO works closely with the various internal legal compliance teams located throughout the world, and specifically with the local data privacy representatives located in each EEA country in which NetApp has an office, that monitor compliance with

the BCRs and the laws on a day-to-day basis. The GCPO is responsible for monitoring compliance globally, and for ensuring that any changes to the BCRs are notified within NetApp operations worldwide and to data subjects whose personal data is collected and processed by NetApp or by a carefully screened partner on behalf of NetApp. The GCPO advises the board of management and the internal Audit Committee, deals with Data Protection Authorities' investigations, reports on compliance with the BCRs annually, ensures compliance at a global level, and manages and coordinates with the local data privacy representatives to ensure compliance with the rules. The local data privacy representatives/responsible parties are responsible for handling local complaints from data subjects, reporting major privacy issues to the GCPO, and ensuring compliance at a local level.

If a data subject, whose personal data is collected, used, and/or processed by NetApp, believes NetApp has not complied with these BCRs, that data subject can contact NetApp's GCPO directly. Data subjects whose personal data is collected, processed, and/or used by NetApp in Europe and transferred outside of the European Economic Area (EEA) may exercise the rights confirmed to them under this BCR against NetApp Holding and Manufacturing BV (NetApp BV), our European legal entity in The Netherlands, in accordance with the terms of our model contracts/transfer agreements (similar to a "Deed Poll'). If the data subject can demonstrate he/she has suffered damage, and can establish facts which show it is likely the damage has occurred because of a breach of our BCRs, NetApp and NetApp BV will accept the burden of proof to show that NetApp was not responsible for the breach of the BCRs that resulted in the damage or that no breach took place.

Our model contracts/transfer agreements bind NetApp, our legal entities, and third party providers listed in the agreements to comply with the BCRs when personal data is collected, processed, used and/or transferred outside of the EEA. The rights and requirements defined in the agreements include:

1) Enforcement of compliance with the BCRs;
2) Lodging a complaint with the relevant European data protection authority of competent jurisdiction and/or to take action against NetApp BV in the courts of the jurisdiction in which the NetApp company responsible for exporting the personal data is established, in order to enforce compliance with the BCRs;
3) Making complaints to a NetApp company within Europe, seek appropriate redress from NetApp BV, including the remedy of any breach of the BCRs by any NetApp company outside Europe and, where appropriate, receive compensation from NetApp for any damage suffered as a result of a breach of our BCRs in accordance with the determination of a court or other competent authority;
4) Obtaining a copy of our BCRs and Model Contracts/Transfer Agreements on request;
5) Rights of the data subjects to enforce the rules as third-party beneficiaries.

Additionally, these BCRs also grant rights to all data subjects to enforce these rules as third party beneficiaries. These rights include judicial remedies for any breach of the rights guaranteed and the right to receive compensation for any breach. These BCRs are governed by and interpreted in accordance with Dutch law. Any supplemental rights or remedies granted to any data subject under the BCRs are enforceable against NetApp Netherlands via the Dutch DPA, the Dutch courts, or other competent Data Protection Authority. Any data subject may report a suspected violation directly to the Dutch DPA, Dutch courts, or other competent Data Protection Authority. If a complaint is filed in another EU jurisdiction outside of the Netherlands, the Data Protection Authority of the EEA country where the complaint is filed has jurisdiction under its applicable data protection law to evaluate the legality of the data transfers by NetApp and its group of companies. In such cases, the Dutch DPA will provide cooperation and assistance,

where required, including providing audit reports available with the Dutch DPA as needed and if relevant.

If a member of the NetApp group outside of the EU violates the BCRs, the courts or other competent authorities in the EU have jurisdiction to enforce action against NetApp. The data subject has the rights and remedies against the member that has accepted liability as if the violation had taken place by it in the member state in which it is based instead of the member of the group outside the EU.

1.9 Responsibility for Liability

NetApp's EU headquarters, NetApp Holding & Manufacturing B.V located in the Netherlands, accepts responsibility for and agrees to take the necessary action to remedy the acts of other members linked by the BCRs outside of the EU and to pay compensation for any damages resulting from the violation of the BCRs by such members of the BCRs. NetApp has sufficient assets to cover the cost and related compensation for any breach and carries $50M in data privacy/data protection and security liability insurance.

1.10 Responsibility for BCR Training

All NetApp employees and alternative workers that have access to any personal data, are involved in the collection of personal data, or involved in the development of products, services or tools used to process personal data are required to complete the NetApp internal data privacy training course, including the BCR training course. NetApp provides various levels of training depending on the amount and type of data collected, accessed, processed, stored, shared and/or transferred. NetApp's training program consists of online data privacy training courses, in-person data privacy classes, and data privacy "brain sharks" that are 10 minute training overviews related to specific data privacy related compliance obligations used as quarterly refresher courses for all employees, All training courses include BCR compliance training.

2 DATA PRIVACY BINDING CORPORATE RULES

2.1 Compliance with the Privacy Laws

NetApp will ensure any personal data on any data subject is collected, processed, used, stored, shared and/or transferred in accordance with local laws.

If there is a situation where our BCRs differ from local laws or regulations, NetApp will always follow the higher standard. These BCRs also apply when NetApp companies process personal data on behalf of other NetApp companies. In situations where NetApp uses third party providers to provide services on our behalf, NetApp requires all third parties to sign our Information Privacy and Security Agreement (IPSA), which hold them accountable for complying with all relevant privacy laws, as well as our internal BCRs. The IPSA is our expanded model contract/transfer agreement.

2.2 Transparency

NetApp will clearly explain to all data subjects why their personal data needs to be collected and how their personal data will be used. We will obtain explicit and unambiguous consents as required by local law and will provide clear and comprehensive notice when personal data is collected describing how personal data will be used and who it will be shared with, unless there is a legitimate basis for not doing so. In the countries requiring consent, NetApp will obtain the consent of the relevant data subjects.

In addition, where a member of the group has reasons to believe that the national legislation applicable to that group prevents the company from fulfilling its obligations under the BCRs and has substantial effect on the guarantees provided by the rules, the member will promptly inform the EU headquarters and the Chief Privacy Officer, except where prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. The Chief Privacy Officer will take a responsible decision on what action to take and will consult with the competent Data Protection Authorities in case of doubt.

2.3 Use of Personal Data

NetApp will only collect, process, use, store, share and/or transfer personal data for purposes which are relevant to NetApp and are known to the data subjects or which are within their expectations.

If NetApp changes the purpose for which personal data is used, NetApp will make data subjects aware of the changes, unless the changes are within the data subject's expectations and they can express their concerns, or unless there is a legitimate legal basis for not doing so. If NetApp changes the purpose for which the personal data is used, NetApp will not process the data in a way that is incompatible with the purposes for which they have been collected. If however, NetApp must process the data for purposes that are incompatible, consent of the data subjects will be obtained. NetApp will identify and clearly explain the purposes for which personal data will be used and who will have access to it.

2.4 Data Integrity and Quality

NetApp will only collect, process, use, store, share and/or transfer personal data that is relevant and not excessive for the purpose. NetApp will keep personal information accurate and up to date. We will only retain personal data for as long as is necessary to meet the purposes for which they are obtained and further processed.

NetApp provides data subjects with a choice of methods to access and amend personal data and communication preferences, including online, in writing, or by contacting the appropriate internal NetApp contact.

NetApp collects, processes and uses the minimum amount of personal data necessary to achieve a valid purpose. We retain personal data only for as long as it is necessary to meet the purpose or other legal requirements.

2.5 Data Security

NetApp has implemented tight technical and organizational security measures to protect all personal data. We apply technical and organizational security measures appropriate to the risks presented by the processing of personal data, and as appropriate to the nature of the data processed. Where NetApp companies process personal data on behalf of other NetApp companies, those companies will adhere to the BCRs and act only on the instructions of the NetApp Company on whose behalf the processing is carried out. Where a third party provider processes personal data on behalf of NetApp or a NetApp company, the third party provider will be required, through a binding contract, to adhere to our BCRs and act only on the instructions of the NetApp company on whose behalf the processing is carried out.

2.6 Data Subject's Rights

NetApp will respond in a timely manner to inquiries or requests made by data subjects about their personal data. NetApp will reply to requests to rectify, delete, block, suppress or cease processing personal data.

A data subject whose personal data is collected and used by NetApp may write to NetApp to ask for a copy of the personal data, including electronic and paper records, about them held by NetApp. If the personal data is inaccurate, the data subject may ask for that data to be corrected, deleted, or blocked, and in certain circumstances may object to the processing of their personal data, if allowable by applicable data privacy laws. NetApp will consider such requests and deal with them as appropriate.

Personal data covered by an access request may include the personal data about the data subject NetApp collects and uses, including a description of the personal data, the purposes for which the data is used, and a description of transfers of that personal data to others. The right of access includes the right to know the source of the personal data held by NetApp. A data subject making an access request can do so in writing to:

Privacy@netapp.com

NetApp, Inc.

Worldwide Data Governance Office

Attn: Ms. Sheila M. FitzPatrick

Chief Privacy Officer

495 E. Java Drive

Sunnyvale, CA 94089

USA

Data subjects can also contact the NetApp office closest to them, which in turn will direct privacy-related enquiries to the Chief Privacy Officer.

NetApp BCRs also grant rights to all data subjects to enforce these rules as third party beneficiaries. These rights include judicial remedies for any breach of the rights guaranteed and the right to receive compensation for any breach. These BCRs are governed by and interpreted in accordance with Dutch law. Any supplemental rights or remedies granted to any data subject under the BCRs are enforceable against NetApp Netherlands via the Dutch DPA, the Dutch courts, or other competent Data Protection Authority.

2.7 Transfer of Personal Data Between NetApp Group of Companies

NetApp processes and transfers personal data relating to the following categories of data subjects:

- NetApp employees, former employees, dependents and beneficiaries of employees, and prospective employees in connection with their working relationships or application for employment (“Employment Data”);
- Our clients and their customers in connection with the sale of products, provision of services, and financial transactions (“Customer Data”);
- Our prospects and leads who have expressed interest in obtaining information related to NetApp products, services and events (“Marketing Prospect Data”);
- Other persons as appropriate to conduct business such as suppliers, partners, contractors, and contingent workers.

The processing and transfers undertaken by NetApp relating to the types of Data Subjects discussed above include processing for the following business purposes:

- Employee Recruitment;
- Employee performance management and professional development;
- Payroll and administration of employee benefits;
- Research and development;
- Business development;
- Maintaining and building upon customer relationships;
- Business planning;
- Facilities management;
- Maintaining technology infrastructure and support;
- Database management;
- Training;
- Maintaining the security of data collected and processed;
- Fulfilling a transaction initiated by or involving a Data Subject;
- Fulfilling a transaction with or for our clients;
- Providing the data to agents and contractors to assist us in our business, some of which may be located outside of the collection country;
- As authorized by applicable laws;
- Fraud prevention or investigation, or other risk management purposes;
- For identification and information verification purposes;
- For protecting NetApp's legal rights or assets;

- Facilitating the acquisition of NetApp businesses;
- Enforcing our rights or the rights of other persons in a financial transaction;
- In response to a lawful request from a court or government agency or to otherwise comply with applicable law or compulsory process:
- On the written request of the Data Subject, where appropriate;
- In emergencies where the health or safety of a person is endangered;
- Other purposes required or permitted by law or regulation.

NetApp processes and transfers a broad range of Personal Data between NetApp entities and to third parties. Third party transfers occur when a third party on behalf of NetApp provides essential services. These services include benefits management, insurance providers, travel services, pension plan management, stock administration, and financial services All third party providers are vetted to ensure compliance with all applicable data protection laws and are required to enter into a standard contractual model clause agreement with NetApp.

The types of Personal Data processes and transfers include:

- Employment Data: This includes data relating to health records, benefit information staff development records, attendance records including any days off due to illness, salary remuneration and expenses information, expatriate information, equal opportunities management, grievance and disciplinary procedures, employee share equity holdings, employment termination information, names, addresses, date of birth, work location, employee performance, trade union membership and next of kin.
- Customer Information: This includes contact information of clients' employees, Information relating to the client's account, clients' customers' contact details including name, address and telephone numbers and account information including other persons on the account and spend thresholds, details of clients' customers' spending and spending patterns and details of the merchants accepting payment transactions to the extent these are individuals.
- Other Personal Data: NetApp also processes contact information of the employees of its suppliers and vendors and independent contractors including name, e-mail address, work location and telephone numbers and such other personal data as may be required in order for NetApp to conduct business with such suppliers, and vendors and independent contractors.

A full description of the main types of Personal Data processed and transferred is available from NetApp’s Corporate Privacy Office.

2.8 Protecting Data Transfers to Third Parties

NetApp will ensure that any personal data transferred to third parties located within or outside of the EEA is adequately protected and processed in accordance with applicable data protection laws.

Transfers of personal data to third parties outside of NetApp or outside of the EEA are not allowed without appropriate steps being taken to ensure there is a legal basis for the transfer and to protect the personal data being transferred. All transfers of data to external controllers located out of the EEA will respect the European rules on transborder data flows in accordance with Articles 25-26 of Directive 95/46EC. For example, NetApp makes use of the EU Standard Contractual Clauses approved by the EU Commission or will use other adequate contractual means in accordance with Articles 25 and 26 of the EU Directive. All transfers of data to external processors located out of the EEA must

respect the rules relating to the processors in accordance with Article 16-17 of Directive 95/46/EU, as well as, the rules on transborder data flows in accordance with Articles 25-26 of Directive 95/46/EC. If a third party service provider processes personal data on behalf of NetApp, either within the EEA or outside of the EEA, NetApp will enter into a contract with that provider which states that the third party service provider will act only on NetApp's instructions and will adopt technical and organizational security measures to safeguard the personal data and comply with relevant data protection laws. Appropriate technical and organizational measures to protect personal data will also be applied during the transfer of the personal data to a third party. Third party providers will also be contractual bound to comply with our BCRs.

Validation of security measures implemented by a third party will take place during the procurement process and will be repeated periodically as required for situations such as contract renewals or changes in business, legal or regulatory requirements.

2.9 Protecting and Limiting Use of Sensitive Data

NetApp will only use sensitive personal data if it is absolutely necessary and where the data subject's explicit consent has been obtained, unless NetApp has a legal basis for using the personal data. NetApp with comply with the legal basis for processing of sensitive data that are enumerated in these BCRs in accordance with Section 6, in Article 8 of Directive 95/46/EC. In accordance with Section 6, NetApp will not process sensitive data unless:

- The data subject has given his explicit consent to the processing of those sensitive data, except where the applicable laws prohibit it; or
- The processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
- The processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
- The processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the Processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or
- The processing relates to sensitive data which are manifestly made public by the data subject; or
- The processing of sensitive data is necessary for the establishment, exercise or defense of legal claims; or
- The processing of the sensitive data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those sensitive data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

Sensitive data is defined as any information related to a data subject's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, medical history, sexual orientation, and criminal convictions. NetApp will assess whether collection and use of the data is required for the proposed use and when it is absolutely mandatory in the context of the business or for legally required purposes. Data subjects must explicitly agree to the collection and use of their sensitive data by NetApp, unless

there is a legal basis for collecting and using the data. NetApp does not collect information related to political or religious affiliation or beliefs or sexual orientation under any circumstances. Collection of race or ethnicity is only collected in a country if, and only if, required under local law for government reporting purposes, but is never transferred or made accessible outside of the country of origination. Information related to criminal convictions is only collected during a pre-employment background check if allowed under local law. The information is reviewed and an employment decision is rendered. Once the employment decision has been made the information is destroyed. NetApp does not store information related to criminal convictions. Information related to trade union membership would only be collected if allowed under local law for legitimate purposes such as payroll deductions for union dues authorized by the data subject. However, at this time, NetApp has no trade unions and therefore the information is not applicable.

2.10 Use of Personal Data for Sales and Marketing

NetApp will not use personal data for direct marketing or sales to a consumer unless that consumer has agreed to that use. NetApp will give all data subjects the opportunity to opt out, free of charge, from receiving direct marketing or sales communications from NetApp, and will respect all opt out requests received. The opt out option will be clearly visible to all data subjects and not buried in a separate document or link.

NetApp will provide data subjects with a choice of methods to access and amend personal data and communication preferences for direct marketing and sales.

2.11 Use of a Privacy Impact Assessment (PIA)

NetApp will require the completion of a Privacy Impact Assessment (PIA) whenever a new system or application is proposed that will impact personal data of any kind. The PIA will help determine the type of personal data that will be collected, used and processed, the purpose of the processing, access rights to the personal data, data storage and/or transfer and the relevant data privacy laws that may be impacted. By using the PIA, NetApp can get in front of any potential data privacy issues and ensure compliance with all relevant data privacy laws before the start of any new project.

2.12 Compliance Audits

NetApp's collection and use of personal data may have significant privacy impacts and therefore are subject to detailed oversight and evaluation through the audit process and on an on-going basis.

NetApp will perform regular audits of compliance to these BCRs. NetApp will ensure these audits address all aspects of the BCRs, including NetApp's information technology systems and databases, security policies, contractual provisions, training, privacy policies, and guidelines.

NetApp will ensure that any issues or instances of non-compliance with the BCRs identified by Internal Audit are brought to the attention of the Chief Privacy Officer, NetApp's company management, and NetApp Inc.'s Board of Directors, and that appropriate corrective actions are taken to ensure compliance.

NetApp will conduct audits of compliance with the BCRs on an annual basis, along with ad hoc audits at the request of the Chief Privacy Officer or a relevant Data Protection Authority. NetApp's Internal Audit Department will coordinate, manage and provide quality assurance of audit work performed by internal or external auditors.

For further detailed information please refer to Appendix 1 – Audit Protocols

2.13 Interaction and Cooperation with Data Protection Authorities

NetApp will provide copies of the results of any audit of the BCRs to any European Data Protection Authority (DPA) of competent jurisdiction, upon request, subject to relevant law. The DPA will respect the confidentiality of the information provided and any trade secrets contained in the information. NetApp's Chief Privacy Officer will be responsible for liaising with the European DPAs for this purpose.

Where any NetApp company subject to the BCRs is located within the jurisdiction of a DPA based in Europe, NetApp agrees that the DPA may audit that NetApp Company for the purpose of reviewing compliance with the BCRs.

Any audit by a DPA will be carried out in accordance with the applicable law of the country in which the NetApp Company is located. In the case of a NetApp company located outside of Europe, the audit will be carried out in accordance with the applicable law of the European country from which the personal data is transferred under the BCRs.

NetApp companies will co-operate and assist each other and the NetApp Chief Privacy Officer when hosting audits by national DPAs. Where required, NetApp will make the necessary personnel available for dialogue with a European DPA in relation to the audit reviewing compliance with the BCRs. Audits will be conducted with full respect to the confidentiality of the information obtained and to the trade secrets of NetApp. NetApp's Chief Privacy Officer will also be responsible for liaising with the European DPA for this purpose.

For additional information please refer to Appendix 4 – Co-Operation Procedure

2.14 Complaint Management

NetApp has a clearly defined process for handling any data privacy-related complaints. If a data subject, whose personal data is collected and used by NetApp, believes NetApp has not complied with the NetApp BCRs, that data subject may raise the matter with NetApp's Chief Privacy Officer. The data subject may also raise the matter with the relevant DPA.

Data subjects whose personal data is collected, processed, and/or used by NetApp in Europe and transferred outside of the European Economic Area (EEA) may exercise the rights confirmed to them under this BCR against NetApp Holding and Manufacturing BV (NetApp BV), our European legal entity in The Netherlands, in accordance with the terms of our model contracts/transfer agreements (similar to a "Deed Poll'). Data subjects entitled to these rights will be notified as part of NetApp's complaints handling procedure.

A data subject can bring a complaint by contacting the Chief Privacy Officer:

- Online at: privacy@netapp.com
- In writing to:

NetApp, Inc.

Worldwide Data Governance Office

Attn: Ms. Sheila M. FitzPatrick

Chief Privacy Officer

495 E. Java Drive

Sunnyvale, CA 94089

USA

- Data subjects can also contact the NetApp office closest to them, which in turn will direct privacy-related enquiries to the Chief Privacy Officer.

The NetApp Chief Privacy Officer is responsible for responding to complaints and working with colleagues from the appropriate NetApp business groups and NetApp companies. NetApp will acknowledge receipt of complaint within 5 working days of the complaint being received by the Chief Privacy Officer. NetApp will respond to a complaint with 30 calendar days of the date the Chief Privacy Officer receives the complaint. If the complaint is too complex to allow a response within 30 days, NetApp will provide the data subject with an estimate (not to exceed 3 months) of when a response will be provided.

The complaint is considered closed on the date NetApp communicates its response to the complaint to the data subject.

If a data subject disputes NetApp's response to a complaint, the Chief Privacy Officer will be notified, and the appropriate resources will be assigned to review the response. After the response has been reviewed, the NetApp Chief Privacy Officer will inform the data subject whether or not NetApp has decided to review the response.

If NetApp decides to review the response, NetApp will promptly inform the individual of the process for carrying out that review. NetApp will respond to the data subject within a reasonable period, which will not be longer than 3 months after the decision to carry out that review. NetApp may need to meet with the data subject as part of the review process. Following completion of the review process, the NetApp Chief Privacy Officer will inform the data subject whether the original response has been upheld or communicate a new response.

NetApp will ensure that any issues or instances of non-compliance with the BCRs identified are brought to the attention of NetApp's Chief Privacy Officer and representatives of NetApp management as required. NetApp will take appropriate corrective actions to ensure compliance.

For further details please refer to Appendix 2 – Procedure for Complaint Handling and Resolution

2.15 BCR Updates

NetApp will inform the relevant DPAs in Europe of any changes to the BCRs. NetApp will provide that information at least once a year of the changes being made. NetApp's Chief Privacy Officer is responsible for communicating changes, and also provides a brief explanation of the reasons for any notified changes to the BCRs. However, NetApp is not obligated to communicate any changes that are administrative in nature or which

have occurred as a result of a change of applicable data protection law in any European country through legislative, court or supervisory authority unless they:

- Result in substantial changes to the BCRs; or
- Affect the authorization of the BCRs by European DPAs.

The NetApp Chief Privacy Officer will maintain an up to date list of the NetApp companies bound by the BCRs. NetApp will send an up to date list of companies to the relevant DPAs at least once a year.

NetApp will communicate the amended BCRs to the NetApp companies bound by the BCRs and will publish the amended BCRs on NetApp's internal and external web sites.

The BCRs contain a change log, which sets out the revision history of the BCRs, including the date the BCRs were revised and the details of any revisions made.

NetApp will ensure that any new NetApp companies are considered for inclusion in the list of NetApp companies bound by the BCRs. NetApp will also ensure that the necessary legal, administrative, operational and technical measures are in place before a transfer of personal data to or from a new NetApp company takes place.

For additional information please see Appendix 5 - BCRs Update Procedures

3 DATA PRIVACY PRINCIPLES

NetApp adheres to the following eight privacy principles:

1) Personal data is processed fairly and lawfully – NetApp only collects and uses personal data for legitimate business needs related to the management of the employment and customer relationships. We do not use the data in ways that have unjustified adverse effects on the data subjects concerned. We are transparent in all aspects of data collection, use, processing, storage, sharing and transferring by clearly articulating the following to data subjects before processing:

    - The identity of the data controller;
    - The purpose of the processing;
    - The recipients or categories of recipients and the purpose for providing the data to the recipients or categories of recipients;
    - Where the data will be stored;
    - and how it will be secured.

    We also provide appropriate privacy notices to data subjects when collecting their personal data. Where required by law, we obtain the prior consent of the data subject.

2) Personal data is processed for specified legal purposes only directly related to the management of the employment and customer relationships – NetApp clearly defines the purpose(s) for which we collect and process personal data and carefully adhere to that purpose(s). We clearly define upfront why we are collecting personal data and what we intend to use that data for. Prior to collection we provide clear notification and where necessary, obtain the consent of the data subject. Data

subject consent is required if the data are to be processed for a purpose incompatible with the purpose for which it has been collected.

3) Amount of personal data held – NetApp ensures that the data collected and processed is adequate, relevant and not excessive in relation to the purpose(s) for which they are processed. We do not collect, process or store more information than is needed for the stated purpose(s).

4) Personal data is kept accurate and up to date – NetApp takes every reasonable step to ensure the accuracy of any personal data we obtain. We ensure that the source of the data is clear and carefully consider any challenges to the accuracy of any information obtained. If notified of any inaccuracies, we immediately correct the data and ensure it is up to date. We regularly validate the accuracy of data to ensure consistency and efficiency through internal audits. Please refer to Appendix 3 – Personal Data Access Requests for an explanation regarding the accuracy of data collected and used.

5) Retaining personal data – NetApp only maintains personal data for as long as is necessary for the specified purpose or purposes or if required by law to retain for a specific period of time. Once the data is no longer relevant or needed, or the employment or business relationship with NetApp has terminated, the data is destroyed unless we are required by applicable law to maintain the data for a specified period of time. NetApp has a strict Records Retention and Destruction Policy that clearly defines the legal retention periods for all data collected, processed and stored. This policy is reviewed on an annual basis to ensure information is only held for as long as needed or for the legally mandated retention period. We continually audit our records to ensure data is updated, archived and securely deleted when appropriate.

6) Personal data is processed in accordance with the rights of the data subjects – NetApp closely follows and monitors our compliance with the laws in regards to the rights of data subjects. We believe these rights to be:

   - A right of access to a copy of all data relating to him/her that are processed
   - A right to object, at any time on compelling legitimate grounds relating to their particular situation, free of charge, to processing of their personal data, unless that processing is required by law. Where the objection is justified, the processing will cease;;
   - A right to prevent processing, free of charge, for direct marketing;
   - A right to object to decisions being taken by automated means;
   - A right have personal data rectified, blocked, erased or destroyed that is inaccurate or incomplete; and
   - A right to claim compensation for damages caused by a breach of the BCRs.

(7) Information security – NetApp takes appropriate technical and organizational measures against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. We accomplish this by designing and organizing our security to fit the nature of the personal data we hold and the harm that may result from a security breach. We also clearly identify who is responsible for ensuring information security and make sure we have the right physical and technical security. We support these efforts through our detailed policies and procedures and enforce the requirement for all employees to be well trained on data privacy requirements and obligations. We have also implemented a

detailed data breach security policy and process in order to quickly and effectively respond to any data security breaches. Access to personal data is strictly controlled and limited based on an individual's job, role and geographical responsibilities. NetApp's Chief Privacy Officer works with each function within NetApp to determine the appropriate access rights within each organization.

(8) Transfer of data outside the European Economic Area (EEA) – As a global company, NetApp does have a legitimate need to transfer personal data outside of the EEA. However, whenever this is necessary, we do provide prior notification to all data subjects and obtain consents when required by law. Additionally we have implemented strict model contracts/transfer agreements both internally and externally, as well as, a data privacy specific confidential non-disclosure (NDA).

4 NETAPP ENTITIES BOUND BY THE BCRS

The following legal entities comprise NetApp, Inc. and NetApp Holding & Manufacturing B.V. and are covered by this Agreement:

NetApp, Inc. (USA)
NetApp Holding & Manufacturing B.V. (The Netherlands)
NetApp B.V. (The Netherlands)
NA Technology CV (The Netherlands)
NetApp Holdings Ltd. (Cyprus)
NetApp Denmark ApS (Denmark)
Decru B.V. (The Netherlands)
NetApp Asia Pacific Holdings, Ltd (The Netherlands)
NetApp Austria GesMBH (Austria)
NetApp Belgium BVBA (Belgium)
NetApp Finland Oy (Finland)
NetApp France SAS (France)
NetApp Deutschland GmbH (Germany)
Network Appliance (Sales) Limited (Ireland)
NetApp Italia Srl (Italy)
NetApp Luxembourg S.a.r.l. (Luxembourg)
NetApp Poland Sp.z.o.o. (Poland)
NetApp Spain Sales S.L. (Spain)
Network Appliance Sweden AB (Sweden)
NetApp UK Ltd. (United Kingdom)

APPENDIX 1 – AUDIT PROTOCOLS

1 Background

The purpose of the NetApp Binding Corporates Rules (Rules) is to establish NetApp's approach to compliance with privacy/data protection laws. This document defines how NetApp's compliance to the Rules will be audited.

The NetApp Worldwide Data Governance Office, and specifically the Chief Privacy Officer, provides guidance about the collection and use of personal data subject to the Rules and analyzes personal data collection and use for potential privacy-related risks. The collection and use of personal data that could pose significant privacy impacts are subject to detailed oversight and evaluation during the audit and on an on-going basis.

2 Approach

2.1 Scope of Audit

NetApp will perform regular audits of compliance to the rules. NetApp will ensure these audits address all aspects of the Rules, including NetApp's information technology systems and databases, security policies, contractual provisions, training, privacy policies and guidelines.

NetApp will ensure that any issues or areas that do not comply with the Rules that are discovered through our audits are immediately brought to the attention of NetApp's Chief Privacy Officer and NetApp executive management (Corporate Officers, and Executive Management Team), and NetApp Inc's Board of Directors, and that appropriate corrective actions are taken to ensure compliance.

2.2 Audit Timeframes

NetApp will conduct regular annual audits for compliance to the rules through our standard data privacy assessment and evaluation process. NetApp will conduct the audits of compliance to the Rules on both an annual and ad hoc basis at the request of our Chief Privacy officer or any other competent function.

2.3 Auditors

NetApp's Internal Audit Department is responsible for undertaking all compliance audits to the Rules. Internal Audit will coordinate and engage with external auditors as needed and will manage and provide quality assurance of all audit work performed.

2.4 Audit Reports for European Data Protection Authorities

NetApp will provide copies of the results of any audit conducted on audits to the Rules any European Data Protection Authority (DPA) of competent jurisdiction upon request, subject to applicable law. The DPA must respect the confidentiality of the information provided in the audit report and protect the confidentiality of any intellectual property or trade secrets that may be contained within the report. NetApp's Chief Privacy Officer is responsible for liaising with the European DPAs for this purpose.

2.5 European Data Protection Authority Audits

Where any NetApp company subject to the Rules is located within the jurisdiction of a Data Protection Authority based in Europe, NetApp agrees that the Data Protection Authority in that jurisdiction may audit that NetApp company for the purpose of reviewing compliance with the rules.

Any audit by a DPA will be conducted in accordance with the applicable law of the country in which the NetApp company is located. If the NetApp company is located outside of Europe, the audit will be conducted in accordance with the applicable law of the European country from which the personal data is transferred under the Rules. The lead DPA shall be informed and/or involved with the audits depending on the nature and/or the outcome of the audit.

NetApp companies will co-operate and assist each other and our Chief Privacy Officer when hosting audits by national DPAs. If required, NetApp will make the necessary personnel available for discussion with a European DPA in relation to the compliance audit to the rules. Audits will be conducted with full respect to the confidentiality of the information obtained and to the intellectual property and trade secrets of NetApp. NetApp's Chief Privacy Officer will also be responsible for liaising with the European DPA for this purpose.

APPENDIX 2 – PROCEDURE FOR COMPLAINT HANDLING AND RESOLUTION

1 Background

The purpose of the NetApp Binding Corporate Rules (BCRs) is to define and establish NetApp's approach to compliance with privacy/data protection laws. This appendix to our BCRs provides an overview of the steps NetApp takes when responding to complaints from individuals regarding NetApp's collection and processing of their personal data.

If an individual whose personal data is collected and processed by NetApp believes NetApp has not complied with our BCRs, that individual may raise the matter with NetApp's Chief Privacy Officer. The individual may also raise the matter with the relevant national data protection authority.

In addition, an individual whose personal data is collected and processed by NetApp in Europe and transferred outside of Europe may also make a claim against NetApp, either in the courts of the European country of the NetApp company that collected and processed the personal data or in the Dutch courts. If a complaint is filed in another EU jurisdiction outside of the Netherlands, the Data Protection Authority of the EEA country where the complaint is filed has jurisdiction under its applicable data protection law to evaluate the legality of the data transfers by NetApp and its group of companies. In such cases, the Dutch DPA will provide cooperation and assistance, where required, including providing audit reports available with the Dutch DPA as needed and if relevant.

Individuals entitled to these rights will be notified accordingly as part of the complaints handling procedure described below.

2 Approach

2.1 Making a Complaint

An individual can bring a complaint by contacting the NetApp Chief Privacy Officer

- Online at: privacy@netapp.com
- In writing to:

  NetApp, Inc.

  Worldwide Data Governance Office

  Attn: Ms. Sheila M. FitzPatrick

  Chief Privacy Officer

  495 E. Java Drive

  Sunnyvale, CA 94089

  USA

- Individuals can also contact the NetApp office closest to them, which in turn will direct privacy-related enquiries to the Chief Privacy Officer in a timely manner.

2.2 NetApp's Response

NetApp's Worldwide Data Governance Office, and specifically the Chief Privacy Officer, is responsible for responding to any complaints, working in closely with colleagues from the appropriate NetApp business groups and NetApp companies. NetApp will acknowledge receipt of a complaint within 5 working days of the complaint being received by NetApp's worldwide Data Governance Office. NetApp will respond to a complaint within 30 calendar days of the date the complaint is received by the Worldwide Data Governance Office.

If the complaint is too complex to allow a response within 30 calendar days, NetApp will provide the individual with an estimate (not exceeding three months) of when a response will be provided. The complaint is considered closed on the date NetApp communicates its response to the complaint to the individual.

2.3 Individual Dispute Process

If a data subject disputes NetApp's response to a complaint, the Chief Privacy Officer will be notified, and the appropriate resources will be assigned to review the response. After the response has been reviewed, the NetApp Chief Privacy Officer will inform the data subject whether or not NetApp has decided to review the response.

If NetApp decides to review the response, NetApp will promptly inform the individual of the process for carrying out that review. NetApp will respond to the data subject within a reasonable period, which will not be longer than 3 months after the decision to carry out that review. NetApp may need to meet with the data subject as part of the review process. Following completion of the review process, the NetApp Chief Privacy Officer will inform the data subject whether the original response has been upheld or communicate a new response.

NetApp will ensure that any issues or instances of non-compliance with the BCRs identified are brought to the attention of NetApp's Chief Privacy Officer and representatives of NetApp management as required. NetApp will take appropriate corrective actions to ensure compliance.

If a data subject whose information is collected and used by NetApp in Europe and transferred to NetApp companies outside Europe is not satisfied with the way a complaint has been handles, the data subject has the right to complain to a European DPA. The data subject may also lodge a claim with a court of competent jurisdiction. Data subjects entitled to such rights will be notified accordingly as part of the complaints handling procedure.
If a data subject disputes NetApp's response to a complaint, the Chief Privacy Officer will be notified, and the appropriate resources will be assigned to review the response. After the response has been reviewed, the NetApp Chief Privacy Officer will inform the data subject whether or not NetApp has decided to review the response.

If NetApp decides to review the response, NetApp will promptly inform the individual of the process for carrying out that review. NetApp will respond to the data subject within a reasonable period, which will not be longer than 3 months

after the decision to carry out that review. NetApp may need to meet with the data subject as part of the review process. Following completion of the review process, the NetApp Chief Privacy Officer will inform the data subject whether the original response has been upheld or communicate a new response.

NetApp will ensure that any issues or instances of non-compliance with the BCRs identified are brought to the attention of NetApp's Chief Privacy Officer and representatives of NetApp management, including NetApp Corporate Officers, Executive Management Team, and Board of Directors as required. NetApp will take appropriate corrective actions to ensure compliance.

A data subject, whose information is collected and used by NetApp in Europe and transferred to NetApp companies outside Europe in a non-compliant manner, has the right to complain to a European DPA or to lodge a claim with a court of competent jurisdiction. Data subjects entitled to such rights will be notified accordingly as part of this BCR.

APPENDIX 3 – PROCEDURE FOR PERSONAL DATA ACCESS REQUEST

1 Background

The purpose of the NetApp Binding Corporate Rules (BCRs) is to define and establish NetApp's approach to compliance with privacy/data protection laws. This appendix to our BCRs provides an overview of the steps individuals can take to ask for a copy of the information NetApp holds on them.

Any individual whose personal data is collected and processed by NetApp may write to NetApp and request a copy of the personal data, including electronic and paper records, about them held by NetApp. This is referred to as a "Request." If the personal data is determined by the individual to be inaccurate, the individual may ask NetApp to correct, delete or block the personal data. In certain circumstances, the individual may object to the processing of their personal data. NetApp will consider all Requests and deal with them as appropriate and in compliance with our BCRs.

This appendix defines the procedure NetApp will follow when we receive a Request.

2 Approach

2.1 Scope of Requests

NetApp will respond to all individuals who make any type of Requests, whether made formally or informally, and whether or not they specifically mention data privacy/protection laws. Personal data covered by a Request may include the personal data about the individual that NetApp collects and processes, including a description of the personal data, the purposes for which the data is used, and a description of any transfers of the personal data to others, both internal and external to NetApp. The right of access includes the right to know the source of the personal data held by NetApp.

2.2 Making a Request

An individual who would like to make a Request can do so as follows:

- Online at: privacy@netapp.com
- In writing to:

  NetApp, Inc.

  Worldwide Data Governance Office

  Attn: Ms. Sheila M. FitzPatrick

  Chief Privacy Officer

  495 E. Java Drive

  Sunnyvale, CA 94089

USA

- Individuals can also contact the NetApp office closest to them, which in turn will direct privacy-related enquiries to the Chief Privacy Officer in a timely manner.

Any individual making a Request is required to confirm that any data they provide when making the Request is accurate (to the best of their knowledge) and to confirm that they are only requesting their own personal data and not that of another person. Requests can be made at reasonable intervals, but not to exceed twice per year unless there is a legal justification for asking more often. NetApp may require a small fee for Requests, but only if allowed by local law.

2.3 NetApp's Response to a Request

NetApp will make every reasonable effort to acknowledge receipt of a Request within 5 working days of the Request being received by NetApp's Chief Privacy Officer. NetApp will explain to all individuals making a Request that it will be necessary to confirm their identity and require more detailed information in an effort to located the requested personal data and to ensure that the individual requesting the data is the individual to which the data relates. NetApp will clearly articulate that attempting to obtain personal data about another person may be a violation of the law.

If the Request is ambiguous, unclear, imprecise or unreasonable, NetApp will require the individual to provide clarity regarding the personal data they are requesting and where they expect this data to be found (if they know). NetApp will reply within 30 calendar days of the date the Request is clearly understood by NetApp. If the Request is too complex to allow a response within 30 calendar days, NetApp will inform the individual and provide a reasonable estimate as to when a response will be provided.

Exemptions and restrictions

NetApp's exemptions to the right of access will not go beyond what is necessary in a democratic society. NetApp will only use exemptions if the following apply:

(a) the exemption constitutes a necessary measure to safeguard national security, defense, or public security;

(b) the exemption is for the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(c) the exemption is for an important economic or financial interest of a State; and

(d) the exemption is for the protection of the data subject or of the rights and freedoms of others;

A Request will be considered closed on the date the individual making the Request is provided with the data or is informed that NetApp cannot provide the data.

2.4 Dispute of a Response

If an individual disputes a response from NetApp, the individual may notify NetApp that they do not agree with the response and/or raise the matter with the relevant national data protection authority. If the individual notifies NetApp that they do not agree with the response, the issue will be handled in accordance with this Complaint Handling process.

APPENDIX 4 – CO-OPERATION PROCEDURE

1 Background

The purpose of the NetApp Binding Corporate Rules (BCRs) is to define and establish NetApp's approach to compliance with privacy/data protection laws. This appendix describes how NetApp companies will co-operate with each other and with the European data protection authorities in regards to our Binding Corporate Rules (BCRs).

The provision of any information under this Co-operation Procedure will be subject to applicable law. The data protection authorities will respect the confidentiality of any data and any confidential or proprietary information, and any trade secrets that may be contained in the information.
This appendix defines the procedure NetApp will follow when we receive a Request.

2 Approach

2.1 Co-Operation between NetApp Companies

NetApp companies will co-operate and assist each other and the NetApp Chief Privacy Officer when handling requests or complaints regarding our BCRs from individuals or from any national data protection authority. NetApp companies will comply with any instructions from the Dutch DPA, Dutch courts or any relevant national data protection authority requiring the remedy of a breach of the BCRs.

2.2 Co-Operation with the European Data Protection Authorities

Whenever and wherever required, NetApp will make the appropriate personnel available for interaction with a European data protection authority in regards to our BCRs. NetApp will actively review and take every reasonable effort to comply with:

- Any decisions made by a relevant European data protection authority on any data protection law issues that may impact the BCRs; and
- The views of the Article 29 Data Protection Working Party as defined in its published guidelines on Binding Corporate Rules.

NetApp will comply with any formal decision of the applicable data protection authority on any issues related to the interpretation and application of our BCRs where a right to appeal is not exercised.

2.3 European Data Protection Authority Audit

NetApp will, upon request by a European data protection authority of competent jurisdiction, provide that authority with a copy of the results of any audit of our BCRs under our Audit Protocols found in Appendix 1 of this document.

Where any NetApp company subject to the BCRs is located within the jurisdiction of a data protection authority based in Europe, NetApp agrees to that data protection authority audit the NetApp company for the purpose of reviewing compliance with the BCRs.

Any audit by a data protection authority will be conducted in accordance with the applicable law of the country in which the NetApp company is located. If a NetApp company is located outside of Europe, the audit will be conducted in accordance with the applicable law of the European country from which the personal information is transferred under the BCRs.

Audits will be conducted with full respect to the confidentiality of the information obtained and to the confidential and proprietary information of NetApp and its trade secrets. NetApp's Chief Privacy Officer will be responsible for coordinating and interacting with the European data protection authorities for this purpose.

APPENDIX 5 – BCRs UPDATE PROCEDURE

1 Background

The purpose of the NetApp Binding Corporate Rules (BCRs) is to define and establish NetApp's approach to compliance with privacy/data protection laws. This appendix describes how NetApp will communicate changes to the BCRs to the European data protection authorities, NetApp companies, and to individuals.

2 Approach

2.1 Notifying the Data Protection Authorities of Changes to NetApp's BCRs

NetApp will inform the Dutch Data Protection Commissioner and any other relevant European data protection authorities of any changes to the BCRs. NetApp will provide the information within a reasonable time of the changes being made. NetApp's Chief Privacy Officer is responsible for communicating any changes to the BCRs, along with a brief explanation of the reasons for any changes to the BCRs. However, NetApp is not obligated to communicate any changes that are administrative in nature or which have occurred as a result of a change of applicable data protection law in any European country through any legislative, court or supervisory authority measure unless they result in a substantial change to the BCRs, or affect the authorization of the BCRs by European data protection authorities.

NetApp's Chief Privacy Officer will maintain an up-to-date list of the NetApp companies bound by the BCRs. NetApp will send an up-to-date list of companies to the Dutch Data Protection Commissioner and any other relevant European data protection authorities annually or if requested to do so more often by the Dutch Data Protection Commissioner or any other relevant European data protection authorities.

2,2 Notifying NetApp Companies of Changes to the NetApp BCRs

NetApp will notify all NetApp companies bound by the BCRs of any amendments or changes made, and will publish the amended BCRs on NetApp's internal and external websites. The external website is available at www.netapp.com.

The BCRs contain a change log that maintains the revision history of the BCRs, including the date the BCRs were revised, and the details of the revisions made.

2.3 Inclusion of New NetApp Companies

NetApp will ensure that any new NetApp company is considered for inclusion in the list of NetApp companies bound by the BCRs. NetApp will also ensure that the necessary legal, administrative, operational, and technical measures are in

place before a transfer of personal data to or from a new NetApp company occurs.

2.6 Revision History

Version	*Date Changed*	*Summary of Changes*
1.0	4/12/12	First draft
2.0	7/10/12	Second draft – changes highlighted
3.0	1/18/13	Third draft - Legal entities added
4.0	9/6/13	Fourth draft – Legal organization change
5.0	10/13/14	Fifth draft – changes requested by Dutch DPA
6.0	12/12/14	Final version for Co-Reviewers
7.0	060315	Updates per Dutch and Bavarian DPAs
8.0	061015	Updates per the Dutch and Bavarian DPAs
9.0	081215	Updates per the French DPA. BCRs given final approval by Primary and Co-Reviewers.