NetApp’s Binding Corporate Rules

Originally developed as a response to the European Union’s invalidation of the U.S. Safe Harbor agreement for the transfer of personal information, Binding Corporate Rules have been codified by the GDPR as a legal means of transferring personal data from the EU to the United States.

WHAT ARE BINDING CORPORATE RULES?
Binding Corporate Rules (BCRs) are sets of rules that govern internal corporate handling of personal information. The EU Commission recognizes BCRs as evidence that a company has put in place the underlying policies, codes of conduct, processes, training, audits, and controls related to the proper treatment of personal information with respect to individual data subject rights under the General Data Protection Regulation (GDPR).

BREAKING DOWN NETAPP’S BCRS
NetApp operates in multiple locations around the globe to serve its international and multinational customers. Our BCRs define our corporate approach to the fundamental principles of global data privacy laws, and they specifically address concerns about how data is moved across borders. NetApp adopted its original BCRs long before the GDPR was even contemplated. When the GDPR came into effect, we amended our BCRs to address its requirements for NetApp as a controller and also adopted new BCRs to address our role as a processor in certain of our more recent product offerings. But more critically than the legal requirements of GDPR, NetApp’s BCRs are more than just a document—they are a reflection of our culture.

Our commitment to the common principles of data protection and privacy are made binding in our BCRs. This means that there are enforceable corporate policies and procedures as well as contracts and agreements when relationships preclude other means of enforcement. We are also sensitive to the general distrust of “self-regulation” in the technology industry, so our BCRs commit to external enforcement rights, specifying our accountability to the Dutch supervisory authority (the Autoriteit Persoonsgegevens, which we refer to as the “Dutch SA”) due to our main establishment in Europe being in the Netherlands. We also assure both our customers and our regulators that we have the necessary resources to address a data breach, committing in the BCRs to maintain assets sufficient to cover the costs of a data breach.

THE COMMITMENTS IN OUR BCRS

Legal compliance
We commit to complying with applicable laws in our treatment of personal data. Although this seems simple, any of us who have had to manage huge troves of data know that a lot goes on behind the scenes to make such a broad commitment. The BCRs commit NetApp to our Privacy Principles and to the authority of the Dutch SA.

Transparency
We commit to transparency. We commit to providing you—our customers, partners, and employees—with easily accessible and understandable information about our data practices. For example, our Privacy Policy clearly explains why and how NetApp collects and uses personal information. We provide additional information to our employees inside the NetApp intranet. And, for customers who use NetApp® services to process data that they have collected, NetApp provides commitments on how we process and use that information in our Customer Data Processing Addendum, included in our services contract. We may also provide additional information at our conferences and events, and we are continually improving our communications and documentation to address new and ongoing needs for transparency.

Security
NetApp takes security seriously. Really seriously. We know that you are trusting us with your most valuable asset—your data. The BCRs commit NetApp to technical, organizational, and administrative policies, procedures, and controls designed to provide confidentiality, integrity, and availability of personal information in accordance with the GDPR requirements. But our commitment to security is not just captured in our BCRs—we also commit to security practices through our contracts and service level commitments. Additionally, NetApp security is more than a static commitment—we maintain a dynamic security process, evolving to meet the ever-changing threat landscape.

Individual access
We make it easy for data subjects to exercise their rights under the GDPR, file a complaint about our privacy practices, and get answers to questions about how we manage personal information. You can send email, send letters through the postal service, or call (1-877-263-8277) to initiate a request. Or just contact your local NetApp office and they’ll put you in touch with the right team to help.
Cross-border transfers
NetApp BCRs commit us to when, how, and why we transfer personal information across borders. Most of our cross-border transfers are related to how we share information about our employees in order to provide corporate services for our global workforce. However, our BCRs also bind us to when, how, and why we transfer information about our partners and customers. For example, they bind us when we send information to a payment processor to fulfill an order, send information to our security teams to verify the operational security of our cloud services, or even coordinate with any recipient of personal information to fulfill a data subject request under the GDPR.

Third-party sharing
NetApp also commits to protecting data when it is transferred to any third party, regardless of location. Our security commitments cover all of our practices, including the movement of information across borders. We have policies and processes to vet our supply chain, helping to make sure that we know who we're doing business with and that we can trust them with personal information. In addition to this vetting process, we also have policies and processes in place to include standard contractual clauses in our service provider contracts, to ensure that we can enforce our high standards for privacy and data security.

Sensitive personal information
NetApp commits to restricting access to sensitive personal information, which includes information about a person's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, medical history, sexual orientation, and criminal convictions. For the most part, NetApp commits to not collecting this data. Of course, if the collection of the data is necessary—for example, some laws require us to collect and analyze sensitive personal information in order to comply with antidiscrimination laws—then it is collected, maintained, and disposed of under the applicable standards and with clear disclosures.

Marketing
Like most companies, NetApp creates and shares marketing materials to inform our customers and potential customers of our products and services. Our BCRs ensure that you can always opt out of receiving these marketing communications without cost or penalty.

Accountability
We hold ourselves accountable to these commitments through regular audits. NetApp was also one of the first U.S. companies to go through the comprehensive process of having our BCRs reviewed and approved by the Dutch SA, and we continue to work with the Dutch SA as we evolve our processes and BCRs with the evolution of the law. NetApp cooperates closely with our supervisory authority to help ensure a common culture and understanding around the policies, practices, and controls relating to our customers’ privacy. We provided our most recent updates in April 2019, and we look forward to working with the supervisory authority as we grow our technology offerings and understanding of privacy.