Destiny's Services Privacy Policy

Scope

This policy covers the privacy practices that Destiny Technologies, LLC and its subsidiaries and affiliates ("Destiny" or "we") employ when providing support, consulting, Cloud or other services (the "services") to its customers ("you" or "your"). Destiny established this privacy policy in order to clarify that the use of information to which it may be provided access in order to provide services is more limited than the use of information covered by Destiny's general privacy policy.

Customer Information and Services Data

Customer Information is information that we may collect from your use of the Destiny Web sites and your interactions with us offline. We deal with customer information according to the terms of our general privacy policy.

Services Data is data that resides on Destiny, customer or third-party systems to which Destiny is provided access to perform services (including Cloud environments as well as test, development and production environments that may be accessed to perform Destiny consulting and support services). Destiny treats services data according to the terms of this policy, and treats services data as confidential in accordance with the terms of your order for services.

To illustrate the difference between customer information and services data, when a customer contracts with Destiny for Cloud services, the customer provides information about itself, including its name, address, billing information, and some employee contact information. Destiny may also collect other information about the customer and some employees, for example through its web sites, as part of that interaction. All of that information is customer information, and is treated according to Destiny's general privacy policy.

In contrast, having contracted with Destiny for Cloud or other services, the customer provides Destiny access to its production, development or test environment, which may include personal information about its employees, customers, partners or suppliers (collectively "end users").

How Destiny Collects and Uses Services Data

Below are the conditions under which Destiny may access, collect and/or use services data.

To Provide Services and to Fix Issues. Services data may be accessed and used to perform services under your order for support, consulting, Cloud or other services and to confirm your compliance with the terms of your order. This may include testing and applying new product or system versions, patches, updates and upgrades; monitoring and testing system use and performance; and resolving bugs and other issues you have reported to Destiny. Any copies of services data created for these purposes are only maintained for time periods relevant to those purposes.

As a Result of Legal Requirements. Destiny may be required to retain or provide access to services data to comply with legally mandated reporting, disclosure or other legal process requirements.

Destiny may transfer and access services data globally as required for the purposes specified above. If Destiny hires subcontractors to assist in providing services, their access to services data will be consistent with the terms of your order for services and this services privacy policy. Destiny is responsible for its subcontractors’ compliance with the terms of this policy and your order.
Destiny does not use services data except as stated above or in your order. Destiny may process services data, but does not control your collection or use practices for services data. If you provide any services data to Destiny, you are responsible for providing any notices and/or obtaining any consent necessary for Destiny to access, use, retain and transfer services data as specified in this policy and your order.

Access Controls

Destiny's access to services data is based on job role/responsibility. Services data residing in Destiny-hosted systems is controlled via an access control list (ACL) mechanism, as well as the use of an account management framework. You control access to services data by your end users; end users should direct any requests related to their personal information to you.

Security and Breach Notification

Destiny is committed to the security of your services data, and has in place physical, administrative and technical measures designed to prevent unauthorized access to that information. Destiny security policies cover the management of security for both its internal operations as well as the services. These policies, which are aligned with the ISO/IEC 27001:2005 standard, govern all areas of security applicable to services and apply to all Destiny employees. Destiny's Support, Consulting and Cloud lines of business have developed detailed statements of security practices that apply to many of their service offerings, which are available for review at your request.

Destiny's security policies and procedures are reviewed and overseen by Destiny Global Information Security (GIS). GIS is responsible for security oversight, compliance and enforcement, and for conducting information security assessments and leading the development of information security policy and strategy.

Destiny is also committed to reducing risks of human error, theft, fraud, and misuse of Destiny facilities. Destiny's efforts include making personnel aware of security policies and training employees to implement security policies. Destiny employees are required to maintain the confidentiality of services data. Employees' obligations include written confidentiality agreements, regular training on information protection, and compliance with company policies concerning protection of confidential information.

Destiny promptly evaluates and responds to incidents that create suspicions of unauthorized handling of services data. Destiny GIS and Legal are informed of such incidents and, depending on the nature of the activity, define escalation paths and response teams to address the incidents. If Destiny determines that your services data has been misappropriated (including by a Destiny employee) or otherwise wrongly acquired by a third party, Destiny will promptly report such misappropriation or acquisition to you.

EU Safe Harbor

Destiny is a global corporation, with operations in over 80 countries, and has developed global data practices designed to assure your personal data is appropriately protected. Destiny's privacy practices, including the practices addressed in this policy and those applicable to its services businesses, comply with the United States/European Union Safe Harbor framework and the United States/Swiss Safe Harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data from the European Union member countries and Switzerland. Destiny has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. To learn more about the Safe Harbor program, and to view Destiny's certification, please visit http://www.export.gov/safeharbor/.

If you have any complaints regarding our compliance with the Safe Harbor program, you should first contact us.
Compliance

Destiny has appointed a Chief Privacy Officer. If you believe your services data has been used in a way that is not consistent with this policy, or if you have further questions related to this policy, please contact the Chief Privacy Officer through our online help desk.