Azure e-book series

Microsoft

Turning trust into a competitive advantage

Go beyond GDPR compliance and win customers

Content

01

Introduction

Security. Performance. Reliability.

These are the words you live by when developing apps. With a rash of data breaches and public outcry over how some companies are sharing customer data, privacy should be a primary concern for you, too.

But just how much focus should you put on privacy? Do you meet the minimum bar for legal compliance with regulations like the GDPR and stop there? Or do you make privacy a core principle in everything you do, on par with security, performance, and reliability?

There are numerous other app developers creating solutions and most of them are just as focused as you on the three traditional pillars of development. Not everyone feels the same way about privacy and related regulatory compliance, however. At Microsoft, we've embraced the protection of our customers' data, building privacy into our own solutions and helping our partners like you do the same. In this e-book, we'll discuss why building customer trust is critical to your business. We'll also show you how, by intentionally building privacy into your apps, you can go beyond simply meeting regulatory obligations and turn compliance and customer trust into a competitive advantage. Let's get started.

Who should read this e-book?

This e-book is for database architects and developers who are considering how their database solutions can be compliant with privacy regulations like the GDPR and want to know how to build privacy capabilities into their applications. By reading this e-book, you'll see how embracing compliance as part of your solutions will make your apps more attractive to existing and prospective customers. Plus, this e-book also outlines how the capabilities and features of Azure data services help you build the privacy features your customers want into your solutions.

02

What is the GDPR?

Chances are good that you've received more than one email or viewed more than one article promising to help you comply with the GDPR. But what is it?

GDPR is the acronym for **General Data Protection Regulation**. GDPR is a new privacy regulation introduced by the European Union (EU), and it went into effect in May 2018.

If it's an EU regulation, why do I care?

You care about the GDPR for two reasons:

First, even if your business isn't located in the EU, the regulation probably still affects you.

This is because the GDPR protects any data subject, or person, who resides in the EU. If you have customers, clients, or users who live in the EU, you are required to provide those people with control over how you use their data. In addition, you are responsible for ensuring transparency into how you use the data and for protecting it from breaches.

Personal data, as defined by the GDPR, can include obvious information like name, address, email address, health information, and credit card information. It can also include not-so-obvious information like account IDs, IP addresses, cookies on a local computer, or shopping history.

Ignoring the regulation could be expensive for your company: Fines for non-compliance can range up to €20 million or four percent of your annual worldwide revenue, whichever is greater.[1]

Second, the GDPR is just the beginning of a new wave in privacy and data protection regulations.

The EU is seen as a world leader in privacy issues. As such, EU regulations are the model that other countries choose to follow. Already, countries like Israel and New Zealand are working with the EU to confirm that their regulations are equivalent to EU regulations,[2] so that entities in their countries can easily exchange data with EU entities. What's more, data breaches (and inappropriate sharing of data) are capturing the attention of regulators everywhere, emphasizing the importance of the GDPR and related regulations. That includes the United States,

> A majority of the US public believes changes in law could make a difference in protecting privacy—especially when it comes to policies on retention of their data. 64 percent support more regulation of advertisers and the way they handle personal information.
>
> **– Pew Research Center[3]**

[1] http://eugdpr.org

[2] Mark Scott and Laurens Cerulus. "Europe's new data protection rules export privacy standards worldwide." *Politico*. (January 31, 2018) https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/

[3] "The state of privacy in post-Snowden America." Pew Research Center, Washington, D.C. (September 21, 2016) http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/

where a series of high-profile incidents—involving social media companies, financial institutions, and even the federal government—have captured the concern of constituents and driven regulators to raise the privacy and security banner.

GDPR is an opportunity, not a problem

There's really no doubt that complying with the GDPR is a challenge. With nearly one hundred articles, it's daunting to simply comprehend the entire set of regulations. However, for companies willing to embrace the goals of the GDPR, there is also great opportunity.

The opportunity lies in your ability to use existing technology tools, like those in Microsoft Azure data services, to create competitive advantage. How? By using the process of meeting the GDPR requirements to help you build trust with your existing and potential customers. In turn, this enhanced trust can help to generate new and repeat sales of your applications, products, and services.

Plus, by meeting the GDPR requirements, you'll also reduce the business risks associated with potential data breaches and privacy fiascos like those making headlines in the last few years.

Your customers care

Do customers care about security and privacy? They sure do. A survey by Deloitte[4] shows that consumer confidence fluctuates widely based on a company's use and protection of personal data.

More than half of consumers are less likely to purchase products and services from a company that has had even a single data breach. More than 40 percent will actively avoid companies they feel do not protect their personal information.

In contrast, almost 50 percent are more likely to purchase from companies they believe are protecting their information. Further, 18 percent are willing to pay a **premium** when they think their information is being protected.

Your accountant cares

Customers aren't the only ones who care about your ability to protect personal data. Your accountant cares; your CFO cares; your shareholders care.

Your P&L cares, too. It's expensive when you fail to adequately protect personal data. By 2019, it's expected that data breaches will cost $2.1 trillion USD globally. The average cost of a single data breach will exceed $150 million USD in that same period.[4]

If a breach does occur, being able to react quickly and appropriately can mitigate the damage. The same Deloitte study found that consumers can also show leniency: 51 percent would be forgiving of a single data breach "as long as the company quickly addressed the issue."

Not collecting data is not an option

Let's face it, you can't afford to not collect data about your customers. That data represents competitive advantage, too. Whether you're performing targeted marketing through mobile advertising, running a loyalty program, or simply using customer insights to drive product development, collecting data about your customers is essential to future success.

> Every problem is an opportunity in disguise.
>
> **– attributed to John Adams**

[4] Pat Conroy, Frank Milano, Anupam Narula, and Raj Singhal. "Building consumer trust." Deloitte University Press. (2014) https://dupress.deloitte.com/content/dam/dup-us-en/articles/consumer-data-privacy-strategies/DUP_970-Building-consumer-trust_MASTER.pdf

[5] "Cybercrime will cost businesses over $2 trillion by 2019." Juniper Research, Hampshire, UK. (May 12, 2015) https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

Great!
You're convinced.

- Because you're a consumer, too.
- You can also see why customers would choose your products and solutions over a competitor's as long as you can show you're protecting their data.
- Plus, you don't want to be hit with the expense of a data breach, in either direct costs or lost sales.
- Oh, and you don't plan to stop collecting customer data, either.

So, what's the first step?

GDPR compliance is your first step

This is where GDPR compliance can help. You can use the process of complying with the GDPR requirements to ensure that you're adequately protecting your customers' data. Once you know you're protecting their data, make sure your customers know by sharing some details with them.

Microsoft has a compliance model to help you through the process, and Azure includes tools and capabilities to make the work even easier.

03

Simplify compliance with Microsoft and Azure

Let's start with our recommended compliance model, which focuses on these three steps:

1. **Assess and manage compliance risk.**
2. **Protect personal data.**
3. **Streamline processes.**

In the following sections, we'll cover these steps in more detail and discuss Microsoft and Azure tools that can help along the way.

Assess and manage compliance risk

The first step is understanding your level of compliance risk and knowing where to make changes. If you aren't sure which compliance standards apply to you, you're not alone. We recently polled our customers, and 47 percent of executives surveyed said they were unsure of what data compliance standards applied to their organizations.[6]

We know that tracking compliance can be difficult, especially when you're addressing more than just GDPR requirements. Microsoft created Compliance Manager to help you assess your current compliance state and manage the process as you increase compliance.

Simplified oversight with Compliance Manager

A web-based solution for meeting data protection and compliance requirements, Compliance Manager:

- Helps you perform **real-time risk assessments** of Microsoft cloud services like Azure Data Services.
- Provides recommended **action items** to help you improve data protection capabilities.
- Includes built-in **reporting tools** you can use for audits and control management.

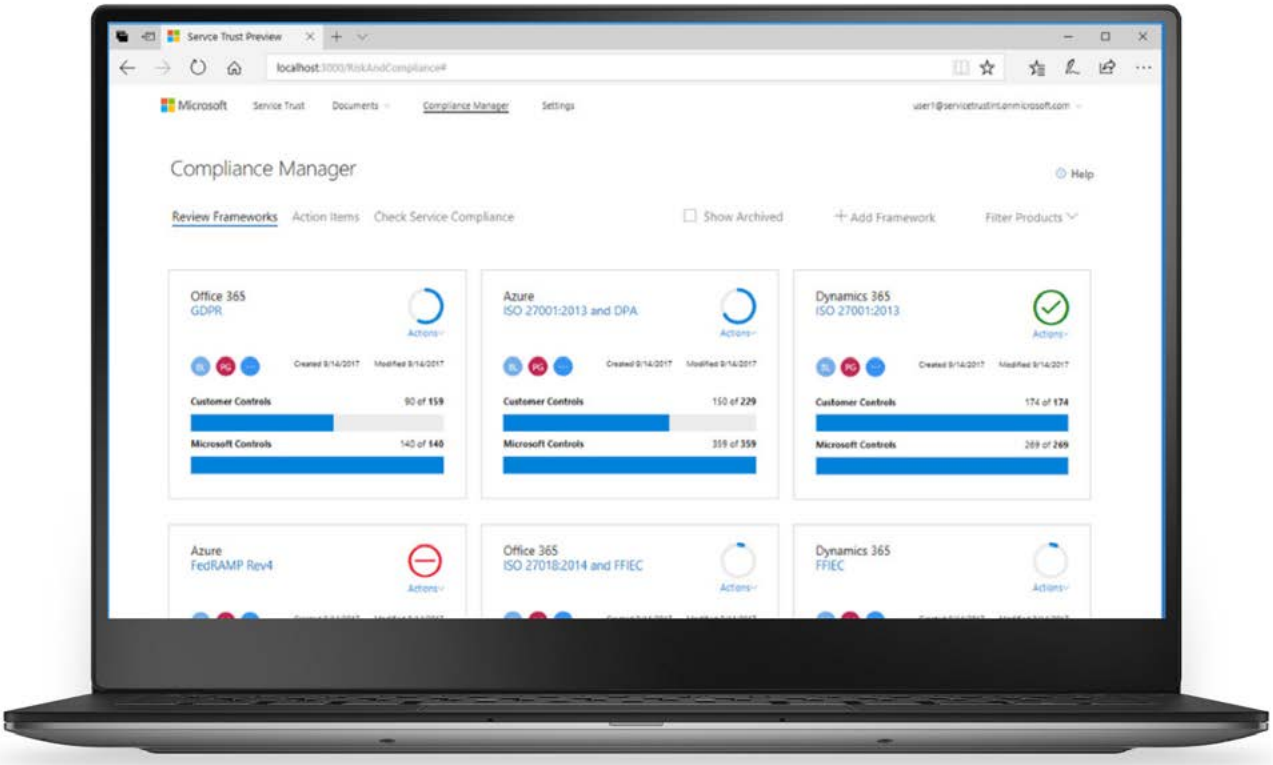
[6] Microsoft GDPR Survey – November 2017

For GDPR, specific dashboards help you track adherence to 118 separate compliance controls, which are mapped to the text of GDPR articles. This includes Microsoft-managed controls that Microsoft is responsible for as a data processor, as well as customer-managed controls that you are responsible for as the data controller. With these dashboards, you can set your compliance status, provide details about your controls, and even upload artifacts like process documentation.

In addition, keep in mind that Compliance Manager is designed to help you manage compliance for more than GDPR. It can help you with a wide variety of compliance standards, including NIST 800-53, ISO 27001, and ISO 27018. As you focus on turning compliance into your competitive advantage, it will be invaluable to show compliance with these standards as evidence of your trustworthiness.

SQL Vulnerability Assessment

You can also use the SQL Vulnerability Assessment to help you determine your compliance risk. We'll talk about this in more detail later in this e-book.



Protect personal data

The overall goal, of course, is to protect customer data. This is what your customers value, and it's the objective of the GDPR and other compliance regulations. But how can you make sure you're protecting all that data? We've found that data protection is further broken down into four steps:

1. **Discover** personal data and where it resides.
2. **Manage** how personal data is used and accessed.
3. **Protect** personal data by establishing security controls to prevent, detect, and respond to vulnerabilities and breaches.
4. **Report** on personal data, systems, and processes so you can retain required documentation, manage data requests, and provide breach notifications.

Knowing this process, Microsoft has developed tools and technologies to help with each step.

Discover

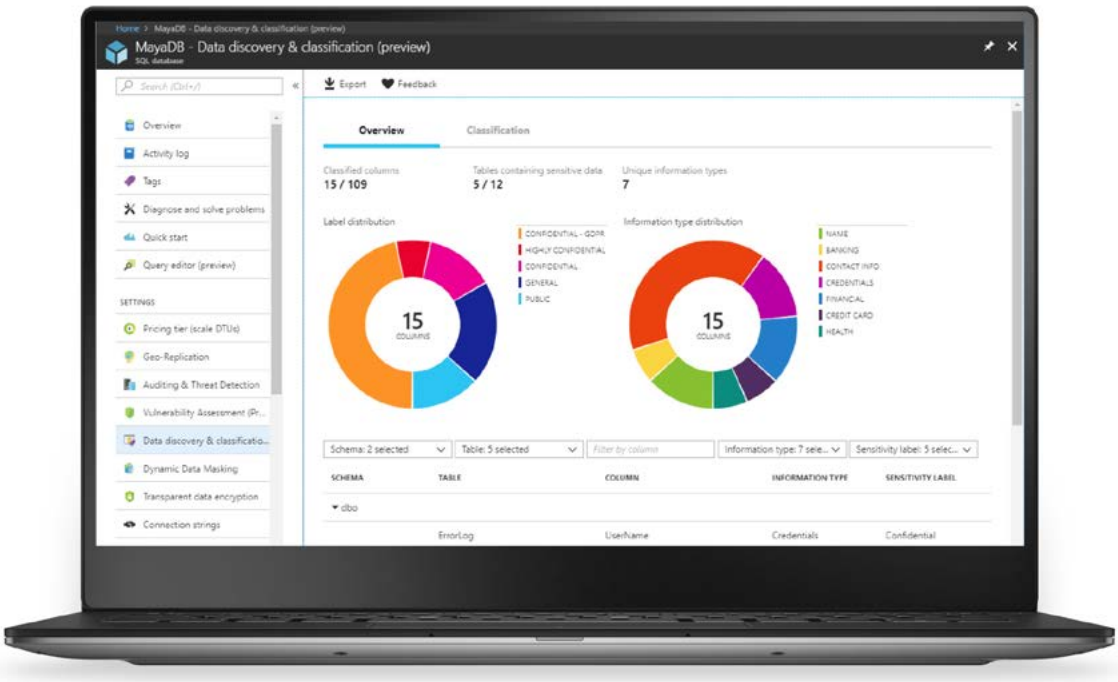
In the Discover step, you identify the customer data you have and where it resides in your systems. The following Azure Data Services tools and technologies can help you with discovery:

Data Discovery and Classification

Data Discovery and Classification is a new tool built into Azure SQL Database and SQL Server Management Studio for discovering, classifying, labeling, and reporting on sensitive data in your databases. Key features include two metadata attributes that apply to columns:

- Labels: Used to define the sensitivity of data.
- Information types: Used to provide additional granularity into the types of data stored in a column.

Data Discovery and Classification helps you automatically discover and classify sensitive data and persistently tag it with sensitivity labels like Business, Financial, Healthcare, or Personally Identifiable Information (PII). It also enables you to control access to data based on classification, which is an important capability for the Manage step, discussed below.



Azure Data Catalog

Azure Data Catalog is a fully managed cloud service that enables you to register sources of data in your organization, making them easier to discover. It helps you build a strategic platform for GDPR compliance by providing capabilities for discovering personal data via search, indexing and searching metadata, and even annotating data sources.

Full-text search

Azure SQL Database supports full-text search, where your users and applications can run full-text queries against any character-based data in SQL Server tables. This includes the use of CONTAINS and FREETEXT predicates and rowset-valued functions like CONTAINSTABLE and FREETEXTTABLE when using the SELECT statement. With full-text search, you can search tables to discover words, word combinations, or variations of a word such as synonyms or inflectional forms.

Manage

The Manage step is all about governing how personal data is used and accessed. In addition to Data Discovery and Classification, Azure's data services provide many other features to help you control data access.

Azure AD and SQL Server authentication

With Azure Active Directory (AD) and SQL Server authentication, you can manage the identities of users who can access databases and servers and prevent unauthorized access. Each authentication solution has its own benefits and limitations.

Object-level permissions

Object-level permissions allow you to grant permissions at an exceptionally granular level—down to table view, stored procedure, scalar function, or service queue.

Role-based security

With role-based security, you can assign permissions based on role or group of users, instead of to individuals. This reduces the attack surface for your database and simplifies security administration.

Row-level security

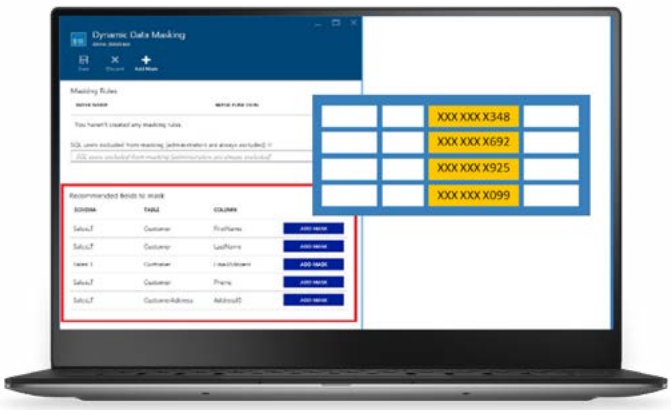
Row-level security restricts access according to specific user entitlements. This means you can limit access to rows in a table based on the relationship between the user and that data.

Azure SQL Database firewall

The Azure SQL Database firewall is a cloud service that lets you limit access to a database server to a specific set of computers, based on originating IP address. This includes the ability to specify subnets within your virtual network. In total, the firewall service helps to ensure that only authorized connections can get to your data.

Dynamic data masking

Dynamic data masking (DDM) limits exposure to sensitive data by masking it from non-privileged users. It masks data in real time, making design and coding of security in applications easier. It also lets you locate potentially sensitive data, helping with the Discover stage.



Protect

For the Protect step, you establish security controls to prevent and detect intrusions and vulnerabilities. When issues do occur, these controls also allow you to respond quickly. In addition, an important part of data protection is making sure data is accessible when needed, for both reporting and legitimate uses. Azure Data Services tools can help you protect data in all these ways.

Transport Layer Security

Azure data services support Transport Layer Security (TLS) 1.2 for highly secure communications. Data is encrypted to help ensure it's not intercepted during transit to or from your database.

Transparent Data Encryption

Transparent Data Encryption (TDE) helps protect against the threat of malicious activity by performing real-time encryption and decryption of databases, backups, and transaction logs without requiring any change to your applications.

Auditing and threat detection

Auditing and threat detection for Azure SQL Database tracks database activities to help you understand and identify potential threats, suspected abuse, or security violations. Threat detection continuously profiles and monitors application behavior and notifies the database administrator of suspicious activity.

Always Encrypted

Always Encrypted is a technology that helps protect sensitive data both at rest and in transit. It makes encryption transparent to applications by encrypting sensitive data inside client apps without revealing encryption keys to the database engine.

Always On Availability Groups

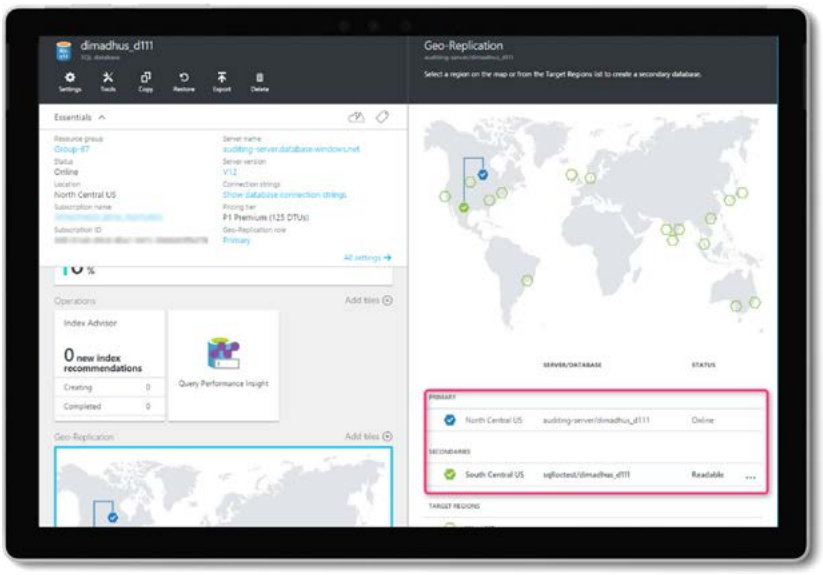
Always On Availability Groups help provide a high availability and disaster recovery solution as an alternative to database mirroring. This ensures resiliency and availability of data during adverse events.

Active Geo-Replication

With Active Geo-Replication, Azure SQL Database can configure up to four secondary databases in the same or different regions, providing database-level recovery in a short period of time. Along with delivering a complete solution for business continuity and disaster recovery (BCDR), Active Geo-Replication can support load balancing and offloading read-only workloads.

Point-in-time restore and long-term retention

Azure SQL Database supports point-in-time restore, thanks to automated periodic backups. As part of Azure Recovery Services, long-term retention is also supported. This means you can store and recover data for up to 10 years.



Report

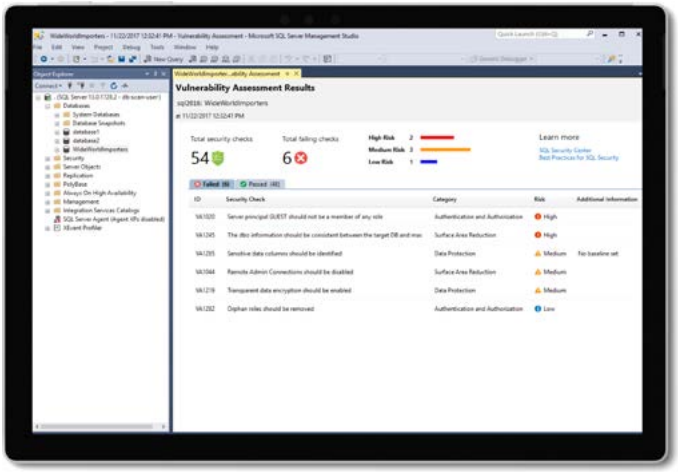
The Report step involves keeping required documentation, managing data requests, and handling breach notifications—all of which are vitally important for compliance with the GDPR and other regulations. We've already seen how Compliance Manager lets you upload artifacts to support your compliance management efforts. Azure also helps with reporting tasks in other key ways.

SQL Server temporal tables

Temporal tables are system-versioned user tables designed to keep a full history of data changes, which you can use for easy reporting and point-in-time analysis. Plus, because all changes are audited, you can readily perform data forensics.

SQL Vulnerability Assessment

A scanning service built into Azure SQL Database, the SQL Vulnerability Assessment provides rules that can flag security vulnerabilities, misconfigurations, unprotected sensitive data, and permissions issues. Not only can you assess your level of risk, but you can also set a security baseline for your environment. Plus, when an issue is detected, you can drill down into database scan reports to find actions for resolution.



Streamline processes

With all four steps to protecting customer data addressed, it's now time to build streamlined processes around that protection. The GDPR requires you to notify the Data Protection Agency (DPA) of any breach within 72 hours. Also, don't forget the Deloitte findings mentioned earlier: Your customers will be more forgiving if you act quickly when something goes wrong.

So, what's your next move? You need to document your processes and conduct practice drills for breaches and data intrusions. Luckily, Compliance Manager and the SQL Vulnerability Assessment were designed to help with both. Just remember that compliance is not a one-time goal that's reached and checked off—it's an ongoing process.

04

Our commitment to you—and your commitment to your customers

You've seen the data and read the findings. It's clear that by creating a business your customers can trust, you can grow sales and promote long-term retention. Systems and processes built around compliance with regulations like the GDPR go a long way toward gaining that trust. Microsoft and data services from Azure help you be successful in your compliance journey. That's why we've provided tools and features to help you along the way. We're also making this pledge to you:

- **We are committed** to our customers' privacy and putting them in control of their data. It is a priority for us to ensure that all our products and services are compliant with applicable law. We'll share our experiences in complying with complex regulations like the GDPR.
- **We and our partners are prepared** to help you meet your policy, people, process, and technology goals on the journey to GDPR compliance.

Get started today

Start building trust with your customers today. Pick your free trial option or learn more about Azure services that help you protect your data:

- Sign up for the Azure SQL Database trial today.
- Have non-relational or NoSQL data? Try Azure Cosmos DB free.
- Looking to move your data to the cloud? Speed your journey with the Azure Database Migration Service.
- Review other data services from Azure, like open-source and big data options.