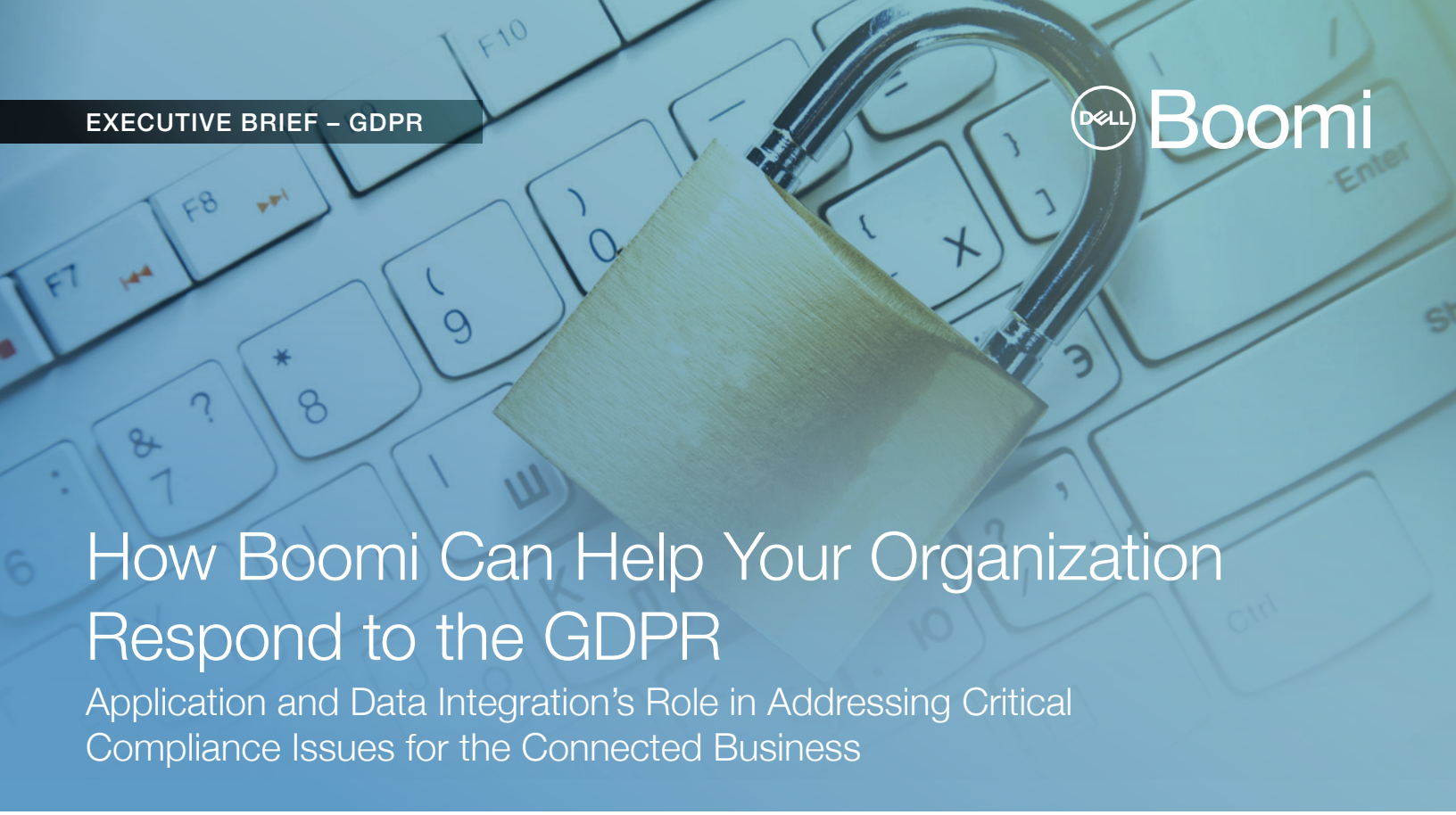
Boomi



How Boomi Can Help Your Organization Respond to the GDPR

Application and Data Integration's Role in Addressing Critical Compliance Issues for the Connected Business

The Future Is Here

The European Union (EU) Data Protection Directive was passed in 1995. However, it didn't — nor could it have been expected to — foresee the massive changes to nearly every aspect of daily life brought on by the evolution of digital technology. An update was needed. And it took the form of the General Data Protection Regulation (GDPR) that went into effect on May 25, 2018.

The GDPR establishes a single set of data protection rules to protect the personal data of EU residents. It also introduces significant fines for non-compliance, including revenue-based fines of up to four percent of total annual worldwide revenues. Moreover, the GDPR makes it considerably easier for individuals to bring private claims against an organization that is a data controller or processor. (Within the language of the GDPR, "data controllers" are generally the companies that direct how and why personal data is processed. "The processors" are generally those companies that process personal data on behalf of the controller.)

Though certainly not a fix for every aspect of the GDPR, data and application integration can play a significant role in how organizations respond to GDPR requirements. Yet, many organizations don't have the necessary data integration capabilities.

What Is the GDPR and Why Does it Matter?

By now, most compliance professionals in large enterprises know the answers to both questions.

In a 2017 speech, information commissioner for the United Kingdom Elizabeth Denham said that boardrooms need to start caring about GDPR compliance. She noted, "The GDPR gives regulators greater enforcement powers. If an organization can't show that good data protection is a cornerstone of their business policy and practices, they're leaving themselves open to enforcement action that can damage their public reputation and possibly their bank balance. That makes data protection a boardroom issue."[1]

1 Data Protection Practitioners' Conference 2017, "Elizabeth Denham's speech at the Data Protection Practitioners' Conference 2017," March 6, 2017; Note: Original script may differ from delivered version; https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/03/data-protection-practitioners-conference-2017/

Impact of the GDPR Goes Beyond the EU

Though an EU regulation, the GDPR demands the full attention of any worldwide organization that processes the personal information of EU-based individuals to offer them goods or services, or to monitor their behavior within the EU. This includes social media, online tracking and data analytics.

Personal information that falls within the scope of the GDPR includes data such as name, physical address, email address, identification number, location data, online identifier, credit card number and health information. Upon request, organizations must give an EU data subject certain access and/or erasure rights.

In a GDPR Pulse Survey[2], PWC found that GDPR readiness is the number one data protection initiative for more than half the multinational companies based in the United States. The regulation's privacy requirements, such as mandatory record keeping, the right to be forgotten, and data portability are especially top of mind for these companies, the survey reports.

But probably the most telling response of U.S. companies to the looming GDPR deadline comes in the form of financial commitment. More than three-quarters of the survey respondents plan to spend $1 million or more on GDPR compliance. A non-compliance fine of as much as four percent of global revenues is a big stick, prompting concerted efforts from the majority of organizations doing business in Europe.

GDPR Compliance: Dealing with Data Flow

GDPR compliance requires an organization to understand how an EU data subject's personal data is collected, used and shared across an enterprise and with any third-party suppliers, vendors or service providers. The data flows of many multi-national organizations might look like airline flight maps. Data flies all over the place. Having a unified data integration platform that allows companies to identify the right data flowing into the right applications, ensure its quality, and integrate it into necessary systems can help businesses follow certain GDPR requirements.

Fundamentally, GDPR compliance is about emphasizing privacy as an indispensable part of the product (or service) lifecycle — whatever that product or service may be. This is a major shift for most organizations whether in the EU or elsewhere.

A scattershot approach[3] will not help companies properly address GDPR, says Brett Hansen, vice president of client software and general manager of data security at Dell. He adds that GDPR compliance cannot be achieved using software alone.

"I'm a technology vendor, so this is going to sound weird coming from me, but my first recommendation is not to immediately go and buy my cool software," Hansen says. "Instead, my advice is to evaluate your environment, understand your risk and then set a strategy. That strategy cannot be created in a vacuum."

Technology Options

It's unlikely that any single technology or technique can fulfill all GDPR requirements. Regardless, data and application integration are critical to responding to the GDPR. Businesses will want to address data silos by integrating disparate data sources and enforcing data governance rules to ensure data is trusted and removed when there is no legitimate purpose to keep it. If your organization doesn't have strong integration capabilities, it could struggle to address the data governance demands of the GDPR.

Fortunately, modern integration technology has come a long way. Using a unified integration platform as a service (iPaaS), an organization can rapidly and hyper-efficiently build out integrations through a low-code, drag-and-drop development environment.

Data quality can also be assured through native master data management (MDM) capabilities. The best of today's cloud-based integration platforms can also support application programming interface (API) management for connecting to external data sources.

2 PwC, GDPR Series, "Pulse Survey: US Companies ramping up General Data Protection Regulation (GDPR) budgets;" https://www.pwc.com/us/en/increasing-iteffectiveness/publications/assets/pwc-gdpr-series-pulse-survey.pdf/learn_more

3 "Dell's Brett Hansen outlines the road to GDPR compliance in the US," Silicon Republic, Nov. 30, 2017; https://www.siliconrepublic.com/enterprise/brett-hansen-dell-gdpr

Boomi Master Data Hub Helps with GDPR Compliance

Dell Technologies has identified six high-risk obligations (see graphic) that organizations must likely meet as they address the challenges of GDPR compliance. Dell Boomi, as one of the Dell Technologies group of companies, has used this framework to assess how its unified platform can help organizations as they prepare for the GDPR.

Boomi Master Data Hub offers organizations the ability to address three of these obligations for GDPR: **record keeping, accountability principle and data retention.**

High Risk GDPR Obligations

Record Keeping
Requires an organization to maintain records of their processing activities (which extends to any vendor that they engage) as well as document the data protection impact assessment that they have undertaken.

Accountability Principle
An organization must demonstrate that they comply with the GDPR data protection principles.

Data Retention
Key to ensuring fair processing. Personal data should not be retained for longer than necessary in relation to the purposes for which they were collected or for which they are further processed.

Data Security and Incident Management
Requires an organization to have appropriate technical and organizational security controls and procedures in place to ensure the secure processing of an individual's personal data as well as notify individuals and/or an EU supervisory authority in the event of a data breach.

Data Minimization
You should only collect and use data in a manner which is consistent with a legitimate business purpose and consistent with the notice provided to the data subject.

Data Subject Rights
Grant individuals the right to access, correct or erase their personal data upon request. An organization must respond to the individual's request within one month.

GDPR Obligation: Record Keeping

Boomi's Master Data Hub helps trace and maintain data lineage across all attributes for the user, providing a framework of the relationships among data stores, locations, channels and types of consent across linked data sources. For every golden record (a superset of attributes that need to be synchronized to all systems integrated through Boomi), Master Data Hub keeps granular data lineage capabilities.

For example, for every update request processed through the Boomi Hub on behalf of an application, Boomi can track that change against the records it keeps within the repository and help the customer ensure the change meets any applicable compliance standards based on a customer's settings.

If an organization's data stewards decide the change is compliant, it can be applied to the records within the repository. The Boomi Hub pinpoints the exact values that are changing and versions the updated record. In this way, there is a comprehensive history of attribute changes for every master record.

GDPR Obligation: Accountability Principle

The Boomi Hub gives customers the ability to set up data governance rules and keep an audit trail of changes that happen in the system. By default, the Boomi Hub adheres to a basic workflow for every change request processed.

The Hub administrator can also set up added data governance policies. The extension of Master Data Hub capabilities through Boomi Flow also lets customers add workflows, such as data change requests, deletion requests and review requests to help ensure compliance.

For every system that's trying to contribute a change, the Boomi Hub can be configured to find at the field level what values are needed for approval and, if a change is detected, whether it needs to be reviewed. Through the Hub stewardship console, which is a standard feature, Boomi quarantines any traffic that does not respect the rules that an organization has put in place.

As a default setting, the stewardship console allows administrators to see into the queue of outstanding requests that need to be approved, review the master records, and drill down to see the history of changes that have been applied to those records. Integration developers can control what master data updates are contributed to the Hub.

Boomi also keeps a series of operational reporting interfaces for any inbound change request that enters the Boomi Hub. These interfaces can be enabled to track how that request maps through the data lifecycle. Is the data enriched or the record updated, or did the request fail to meet established rules? On the outbound side for traffic that leaves the Hub, it offers an operational interface for tracking what is delivered to a target system.

The Boomi Hub can also be configured to enable end-to-end auditing of data traffic, with a historical reporting console that summarizes a series of metrics to ensure the health of master data over time, including how many records fail to meet compliance on a daily basis.

GDPR Obligation: Data Retention

Boomi Master Data Hub can also track the deletion of data from all contributing systems and third-party data sources to aid in compliance with the GDPR's "right to be forgotten" clause. Boomi Hub provides the ability to design customizable fields and validation rules tailored to applications and data sets, which helps prevent the mastering and/or proliferating of extraneous information.

As a delete request is sent through the system, it retires the golden record kept in the stewardship console and persists a delete command through every spoke on the Boomi Hub where that golden record is synchronized. This will occur in near-real-time for every system and data source integrated with the Boomi Hub.

Better Data Hygiene Beyond the GDPR

Good "data hygiene" is critical to routine business activities beyond the GDPR. So, let's take a closer look at the tools the Boomi integration platform offers organizations to help better manage their data — not just for GDPR purposes but for business operations.

How Boomi Handles Customer Data

When Dell Boomi provides services that involve customer data, it is generally acting as a processor and our customer is the controller.

Dell Boomi appreciates that our customers have various internal teams and external partners they share and exchange data with. However, not everyone should have access to sensitive data that flows through such business processes.

With this essential data management and security need in mind, we designed the Boomi integration platform with features that allow companies to control how data is handled. In general, the **View Data** privilege in the Boomi platform is a feature that is always turned on by default. This allows customers to view data and documents in a process reporting page. When **View Data** is on, this information then flows through the Boomi platform (based in the United States).

However, customers can configure custom roles such that personal data contained in customers' production data that passes through an on-premise ("local") Atom, Molecule or Atom Cloud never flows through the Dell Boomi data center in the U.S. The data and logs are stored on the customer's hosted infrastructure either on-premise or in the cloud where the Atom or Molecule is deployed.

Further, if **Purge Data Immediately** is selected within **Atom Management**, data will be purged upon completion of an integration process — ensuring that no data remains that could be viewed through this function. In terms of integration, Boomi facilitates data transmission between either a SaaS or on-premise application through a connector configured to security requirements of the customer.

Configuration Data and Business Data

Boomi distinguishes between configuration data and business data. Configuration data is the information needed to execute the integration process flows that a customer builds inside the platform. Business data is information related to a customer's business (e.g. invoices, orders, contacts, etc.) and is processed by the Boomi Atom, which is our run-time engine. The customer can deploy the run-time engine anywhere — on the customer's hosted infrastructure on-premise or in the cloud.

Our distributed architecture allows customers to bypass the Boomi platform to keep maximum control when processing business data. Business data is not processed on the platform but may be transferred through the platform as requested by the customer via the user interface (**View Data**), using standard encryption protocols.

Securing Customer Data in Transit

To help ensure the security of data in transit, the Boomi AtomSphere integration platform uses stringent data communication security standards. While an Atom, Molecule or private Atom Cloud is running and executing processes, it stores detailed logs and processed documents locally. You can view them on the Process Reporting page in the Boomi platform.

Customers can control how long logs, processed documents and temporary data are stored in the Boomi Atom, Molecule or private Atom Cloud. If an organization processes a large volume of data and wants to conserve disk space, it can reduce the number of days this information is kept (30 days is the default).

Purged logs, processed documents and temporary data are permanently deleted and cannot be recovered. If your organization wants to keep a longer history of documents for audit purposes, use connector operation archiving or write data received and/or sent to another location as part of your process.

Get Your Data House in Order

GDPR is an opportunity for IT teams to conduct a comprehensive review of their existing data privacy and security practices. While Boomi can help your organization with some key GDPR obligations, ultimately, each organization must decide how it will address the GDPR. Only a handful of articles in the GDPR law relate to IT security, but data protection goes far beyond GDPR.

To learn more about Dell Boomi and how Boomi can help support your GDPR efforts, please visit us at Boomi.com today!

Learn more about how Boomi can help you synchronize data across your IT silos
boomi.com/hub

Speak with a
Boomi integration expert

View all customer stories at
Boomi.com/Customers