omnitza

TABLE OF CONTENTS:



# How integrated Enterprise Technology Orchestration can streamline GDPR compliance efforts

## Tracking the digital estate has never been more critical

### Introduction

The General Data Protection Regulation (GDPR) is a European Union law that went into effect on May 25, 2018. It is a broad mandate that describes how organizations must protect personal data and privacy rights of anyone in EU territory. The GDPR not only applies to customer and partner data but also to employee data. Under GDPR, individual EU countries can enforce the law with their own sanctions and fines via Data Protection Authorities.

GDPR affects any company and organization doing business with European citizens and residents, applying to data collected from these people and stored in any EU member state. There is some question as to whether the GDPR will apply to data for EU residents stored outside the Union, however the most conservative approach is to ensure that the organization can apply GDPR compliance to any customer, partner or employee. Another significant variable is that "stored" means where in the cloud information is physically stored, so where your backups are stored (assuming it's remote for business continuity purposes) can create issues with GDPR compliance.

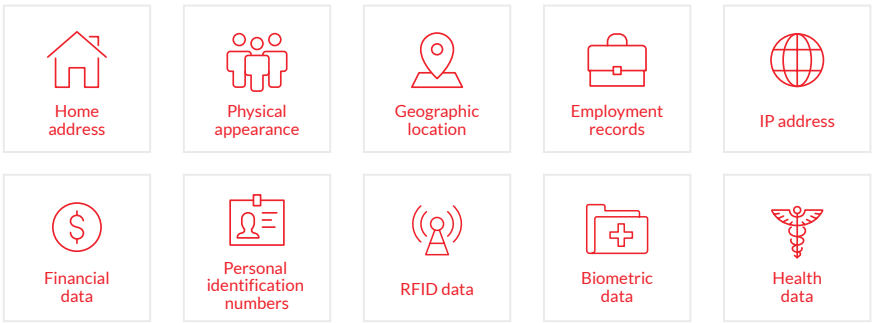
GDPR defines personal data as "...any information relating to an identified or identifiable natural person" (also referred to as a data subject). This might include data on any of *the following attributes:*

Under GDPR, organizations and enterprises must make it easy for consumers to:

- Request and receive all information you have about them
- Correct or update inaccurate or incomplete information
- Request to have their personal data deleted
- Ask you to stop processing their data
- Receive a copy of their personal data in a transferable format
- Object to you processing their data

Similar to the California Consumer Protection Act, (CCPA) the GDPR mandates timely notification in case of a data breach. Unlike CCPA, the GDPR lays out specific financial penalties for non-compliance. Those penalties can be as much as 4% of annual gross revenues, which puts considerable teeth behind the law. Authorities are already using the penalties to enforce the law; in 2019, British Airways was hit with a $230 million fine for a GDPR breach, amounting to 1.5% of the firm's annual gross revenues. (Note: after Brexit, it is unclear whether the UK will continue to enforce GDPR).

Enterprise Technology Orchestration (ETO) plays a critical role in GDPR preparedness and compliance. For example, in the case of a data breach affecting customers of a U.S. company operating in the EU, under

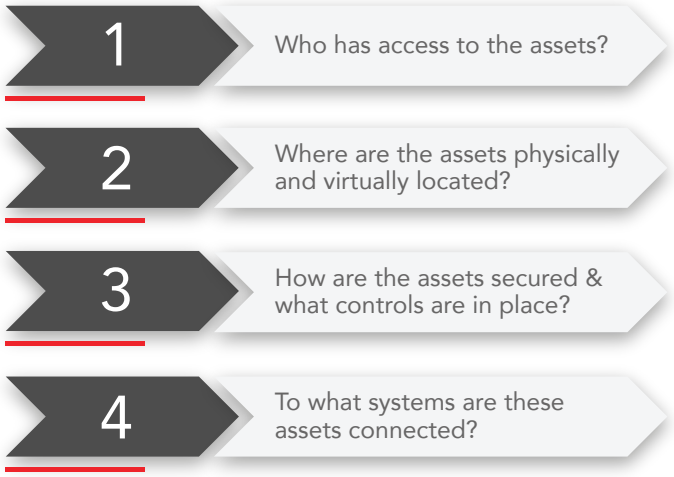


GDPR the U.S. company must identify the source of the breach and all the potential customer records that may have been exposed or leaked. Often breaches are caused by loss of control of physical devices as they transition through their lifecycle, which may have customer data stored onboard or may facilitate access to secured systems. Requests to purge customer information must be completed within specified periods, so not ensuring all instances of a customer's data are removed from all IT assets has a potential nine figure downside.

ETO simplifies tracking and tracing of all IT assets back to users, locations, and IP address activity. IT teams that want to accelerate GDPR response and maximize compliance should proactively con-struct an ETO capability to normalize, track and trace all IT assets across the entire enterprise estate. This capability should enable continuous status updates and data mapping so that an overlay of data flows can be easily applied to allow compliance teams and managers to quickly identify the likely location of data that users are requesting be supplied to them or expunged from their records.

To set itself up for strong GDPR compliance a company should first conduct an exercise mapping all data flows within the company and to third-party partners and service providers. GDPR data managers must know where their customer data is located. However, data maps are underlaid by an understanding of asset management, because the data must reside somewhere. For that reason, GDPR compliance requires a bottoms-up and system-wide accounting of all IT assets under management.

Different legacy ITAM systems, including CMDB, SAM, MDM, SaaS and Cloud infrastructure management, all manage and track key components of what would be reviewed during a GDPR-triggered audit, data request or breach response. Aside from attaining an accurate count of all assets, the ETO must capture the answer to the four key questions:




## Enterprise Technology Orchestration to manage GDPR risk

GDPR risk (and asset management risk more broadly) is becoming more and more complex as the number and type of assets (hardware, software, laptops/phones, Cloud, SaaS) explodes. This new reality highlights the failure modes of most existing static ITAM systems:

- Manual ITAM-centric processes cannot keep up with exponential device and software/SaaS asset growth
- Continuous GDPR compliance requires process-driven yet agile and adaptive track-and-trace of any new asset types
- Redundancy and missing assets in traditional ITAM systems can introduce further risks
- Inability to track and validate the presence of reasonable controls in disconnected ITAM tools may contradict CCPA guidance relative to GDPR and expose legal risk

A comprehensive, accurate, and integrated ETO solution enables a reliable, defensible and efficient GDPR compliance stance. Unlike point solutions and siloed ITAMs, ETO enables automation of key discovery and reconciliation portions of GDPR compliance and response. An ETO system also normalizes data formats across all ITAM types, creating a single database of record that is programmatically addressable and allows export of data via APIs into other systems; this is an important capability for agile and adaptive track-and-trace. Executed properly, ETO offloads large portions of manual GDPR compliance and response into software code and scripts that are easy to update and run on a continuous basis to ensure a current view of the IT estate.

## Use Cases for ETO for improved GDPR compliance and response

ETO has several use cases that can improve, streamline and automate GDPR compliance and response.

### *Rapid response to GDPR data request or breach*

Most mid-sized and large organizations have multiple IT asset management tools and systems, purchased to solve a specific problem (e.g. hardware vs. software). Each tool acquires, stores, structures and updates data slightly differently. Many lack public

APIs (or simply do not have an API) and must be exported as CSV or spreadsheets to integrate with other ITAM data sources. Some automate asset discovery. Some enable scanning of MAC addresses and UUID while others force manual asset information capture by IT personnel. Where systems and tools differ includes:

- Data formats and schemas
- Variety and flexibility of data fields
- Capabilities for data export
- Levels of automation of data capture
- Frequency of updates
- Accuracy and reliability of information
- Capture of asset location and provenance

As a result of these disparities, too frequently IT teams must manually calculate, dedupe and reconcile asset inventories with cumbersome spreadsheets. This causes significant inaccuracies due to human errors and incompatible information, and delivers sub-par results when teams attempt to account for all assets. When an IT team is informed of an Indication of Compromise (IOC), it can take days or weeks to identify the source of the breach as well as its location, owner and all affected systems. Similarly, when an IT team receives a GDPR compliance request to remove or supply all user data, it can be challenging to identify all assets that might be storing or touching pieces of the user's data.

ETO that includes automated data capture and smart reconciliation across siloed asset management systems addresses this issue by automating data capture, mapping fields and schemas into a unified master database, and reconciling across siloed ITAM point solutions to create an accurate, reliable system of record. This system makes it far simpler to formulate and execute a GDPR response to breaches by identifying compromised assets and breach sources. In addition, IT teams can more easily map data flows to real assets, thereby quickly ascertaining which assets contain the relevant information specific to a breach or compliance request. Specifically, ETO's unified system of systematic repeatable data capture and retrieval for the entire digital estate provides:

Higher accuracy of data tracking across asset management systems

Faster response times to GDPR-related breaches and IoCs

Faster and more trustworthy responses to GDPR requests for user data or data deletion

Repeatable, automated, code-driven processes to underpin asset-based compliance

## *How ETO improves GDPR compliance and response*

Installing and rolling out an ETO solution as part of your GDPR strategy is complex but manageable. You should begin by determining the key requirements of GDPR compliance, as well as what you will need to do internally to comply with any GDPR-specific request. You should probably consult with your legal team to get more definition on the specific requirements as you build out your plan; the application of GDPR varies by country and it is a living law open to changing interpretation. With guidance from your legal, audit and security/IT leadership, you should:

**#1. LIST ALL THE SPECIFIC ELEMENTS OF**
*GDPR compliance and associated responses*

**#2. CREATE A PLAN TO MAP ALL DATA**
*flows affecting customer data*

**#3. DECIDE THE END STATE & DESIRED GOAL OF**
*your GDPR exercise. Ideally, this will be an automated reporting capability or dashboard as well as playbooks that can be quickly activated in response to breaches or data requests.*

**#4. ALIGN INTERNAL RESPONSIBILITY FOR**
*ongoing GDPR compliance with your organization chart*

**#5. SPECIFY A DETAILED SCOPE OF WORK REQUIRED TO**
*create effective GDPR compliance and response*

**#6. INVENTORY EXISTING SILOED/ STOVEPIPED**
*asset management systems and their capabilities*

**#7. CALCULATE CURRENT ACCURACY/ COVERAGE RATES**
*of asset management inventories*

**#8. DETERMINE WHAT PARTS OF THE GDPR COMPLIANCE**
*can be automated and what parts must be manual*

**#9. ASSESS WHAT YOUR ETO SYSTEM**
*is capable of delivering in terms of automated reconciliation (ETL, field mapping), discovery (leveraging existing asset management tools), reporting, and data exports (API vs CSV, etc.)*

**#10. CREATE A GDPR COMPLIANCE & RESPONSE WORKBACK**
*plan and jobs to be done, then assign responsibilities*

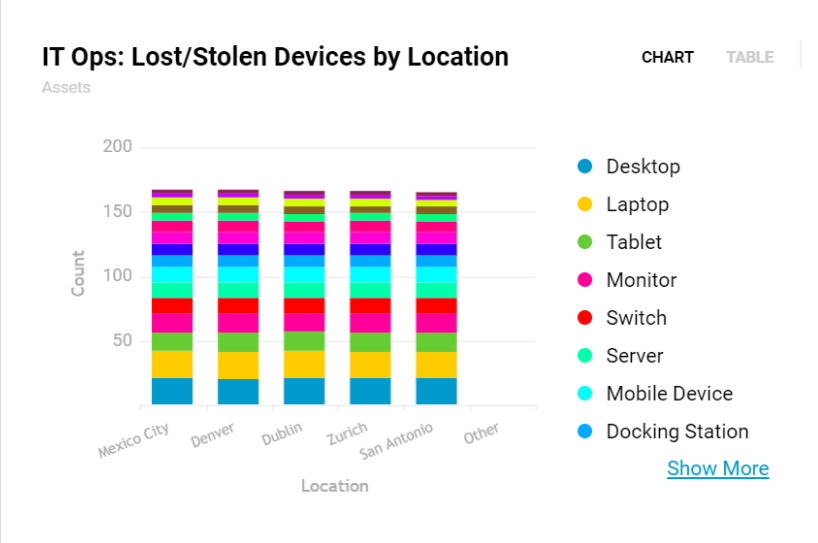
Completing your GDPR planning process will identify gaps and blind spots in asset management information capture and areas for improvement. This can also have broader benefits outside of GDPR, such as enterprise security and employee onboarding. Ideally, your plan should be staged with specific check-ins to ensure that milestones are being met and you are moving towards your desired end-state.

The accuracy and agility of an ETO solution can be critical to project success. Without a programmatic and automated way to establish and maintain an accurate and trustworthy master database of assets under management, all other GDPR response processes are diminished by failings of the underlying data. The best ETOs provide flexible ways (extensibility in modern coding languages like Python JavaScript) to move data into and out of the platform and connect outputs of multiple ITAM tools quickly and easily.

### *Building a business case for ETO for GDPR compliance and response*

Generating a business case for ETO for GDPR is straightforward. Identify the potential risks and costs associated with a breach or penalties for GDPR violations. In a worst case, it could be up to 4% of your gross annual revenues and the EU is not shy about levying fines. This is perhaps the most concrete and concerning risk that your business may face at present. Then consider the benefits you would get in terms of reduced costs and improved processes or saved staff time. Some of these benefits would likely apply beyond GDPR compliance; good data hygiene pays huge organization-wide dividends. Consider benefits such as:

- Savings in staff time responding to data breaches
- Savings in staff time of responding to GDPR data removal requests provenance
- Faster remediation of data breaches
- Reduction in likelihood of horizontal movement of attacks after a breach
- Faster identification of ownership and location of assets




- Rapid response capability for GDPR violations
- Improved prevention of data breaches
- Reductions in staff time spent on manual compliance process
- Faster identification of ownership and location of assets
- Establishing asset management as a real-time competence
- Creating more accurate records of assets company-wide to enhance overall security posture and hygiene

Now calculate your cost/benefits and build a business case for ETO as a core building block for GDPR compliance and response. With a concise and clear before/after picture, approvers will see the potential high GDPR- related costs to the organization of inaccurate, manual and hard-to-update asset management systems. It is also helpful to mention relevant added benefits like increased CISO/C-Suite/BoD confidence in organizational security and compliance. As well, GDPR compliance covers most (if not all) of what is required for California Consumer Protection Act (CCPA) compliance.

Preparing your IT estate for GDPR compliance and ongoing management and response enforces the capability to answer basic and useful questions about your assets: who, where, and what happened? With ETO, you can easily answer these questions and, by extension, all other questions on top of them such as where consumer data is stored and what systems are at risk after a breach. Automating the asset management component of GDPR compliance by connecting incompatible siloed systems, and replacing manual calculations with automated workflows can drive significantly improved GDPR preparedness, while also providing a stronger foundation for better IT asset management and visibility.

## About Oomnitza

Oomnitza is an agentless enterprise technology orchestration solution for digital business. By consolidating technology asset data from siloed systems into a single pane of glass, our customers are able to optimize their technology spend, automate their governance processes to meet compliance and auditing requirements, protect from security risks, and ensure great employee experience and productivity. Oomnitza is headquartered in San Francisco

*www.oomnitza.com*



*© 2021 Oomnitza, Inc. All rights reserved. All trademarks are the property of their respective owner(s). 2/21*