COUNTDOWN TO GDPR: Hidden Data Within My Organization

Data volumes continue to grow despite efforts to reduce digital footprints across the organization. Wherever you look, every part of your organization stores data. Do you know where your EU personal data resides? Can you easily find it, correct it, provide a copy of it to a data subject, or even delete it? As discussed in BDO's GDPR Checklist, the first step is to identify relevant business processes, systems, and data sets likely to contain personal data. The second step is to determine which data sets contain EU personal data belonging to EU "data subjects".

As part of the initial step of identifying relevant data sets, consider where data might be hiding by assessing individual departments and locations. In this article, we identify two buckets for you to consider: "suspected culprits" and "the ones who almost got away". As we have been working through our clients' readiness and implementation steps, we have identified certain departments that consistently store large amounts of data that may be impacted by GDPR that were not effectively considered in the first or second evaluations of the organizations' data.

SUSPECTED CULPRITS

Human Resources

Global organizations with candidates or employees from the EU, would be well served by determining how this data is handled, stored, transferred, managed, and retired. Questions to ask might include: what information do our recruiters retain, how long do they retain it, where is it stored, and who has access to it? Separately, it may be beneficial for the human resources department to work with the legal team to develop GDPR specific records retention and contract language for inclusion in employee contracts and handbooks.

Legal

From contracts, to investigations and litigation documents, to outsourced vendors and law firms, legal departments have a variety of data that contains EU personal data and may also be subject to legal holds. Additionally, your legal team will likely need to develop GDPR specific contract clauses to update vendor and third party contracts to meet the new requirements.

Operations

Systems that are prevalent throughout operations may be point-of-sale (POS) systems, shipping information tied into ERP systems, supply chain systems, or training records. If you are a global organization and collect data from customers or website visitors, you will want to consider all aspects of operations such that these data sets are not overlooked. If you are using a POS system, some questions to consider are: how will we provide data subjects the right to access, view, correct, or delete their information.

Finance

Your organization's accounting platform is ripe with data and the question is whether you have an enterprise-wide ERP system that stores information about EU data subjects. Accounts receivable, accounts payable, and vendor management are just a few areas to consider. If you have global operations, you will want to properly identify organizations and individuals where you may be storing unnecessary data, while balancing GDPR compliance and records retentions policies. Although GDPR is effective on May 25, 2018, there are a number of additional factors for consideration as individual country laws evolve.

THE ONES WHO ALMOST GOT AWAY

Sales, Marketing, and Business Development

Customer Relationship Management, or CRM systems, are an often overlooked source of data within an organization. While many organizations are aware of the systems, it is often unclear how much data is captured in these systems. Additionally, an organization's CRM system typically ties back to a number of other systems or functions such as finance, operations, human resources, POS, and inventory management systems. Establish procedures and reporting into and around these systems for compliance with Articles 15 and 17, Right of Access by Data Subject, and Right to be Forgotten.

IT Departments

It should come as no surprise that IT is a common function to consider. However, while this team manages the storage devices that house different data sources, they may also be responsible for developing GDPR policies and procedures. Since there may be backup locations of data that are unbeknownst to operational areas of the business, it is important to understand how this team manages enterprise data, off-site storage, and backups. You may find that it is necessary to rethink data storage and backup strategies if multiple copies of information are created in the current process.

Third Party Vendors

Digital proliferation has driven companies to use third party vendors to store, process, and manage data for a number of functions throughout the organization. It will benefit your organization to understand data that is accessible by your third parties, how they protect it, if they have physical copies of personal data, and how they will comply with your GDPR obligations. They may be a processor or sub-processor for you so you should also consider contractual obligations that may require modification. Take steps to clean up your third party vendor ecosystem as you embark toward GDPR compliance.

While initiatives surrounding GDPR are normally lead by your organization's Chief Privacy Officer, Chief Information Security Officer, the legal department, or a combination thereof, it is important that every stakeholder have a seat at the table and be part of the conversation. Open and detailed dialogue will help to mitigate risk and enable effective policies and procedures for your organization's systems.

DON'T LET YOUR DATA GET AWAY. For more information about how your organization can effectively work through your data and systems to be compliant with GDPR, contact any member of our national Information Governance Practice or visit www.bdo.com/GDPR.

CONTACT:

KAREN SCHULER
National Data & Information Governance Leader
703-336-1533
kschuler@bdo.com

MARK ANTALIK
Forensic Technology Services Managing Director
617-378-3653
mantalik@bdo.com