IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
Unlimited Validation Knowledge Awaits...
UBM A division of UBM Americas
Published on *IVT Network* (http://www.ivtnetwork.com)

Mastering EU GDPR Compliance: Security and Privacy for Validated Systems

By Valarie King-Bailey Dec 18, 2018 7:12 am PST

Privacy and data protection are more important than ever. Today's headlines are filled with instances of data privacy breaches as well as cyber security breaches among leading global firms. In the European Union a significant regulation has been passed in May 2018 to address the issue of personal data privacy. It is known as the general data protection regulation or GDPR.

Validation engineers each day seek to validate systems across the globe in compliance with current regulatory guidelines. Much of the focus on computer systems validation from a testing perspective is designed to ensure that systems meet their intended use. Installation/Operational/Performance Qualification (IQ/OQ/PQ) is typically conducted by global validation teams to ensure that systems are qualified and to confirm software quality. While the focus for the last 40 years has been on such testing, today's computing environment has changed the paradigm of how we established computing systems environments and validate them. This white paper will focus on today's challenges and how validation engineers must address the changing system landscape and not only deal with issues concerning data privacy but those of Cybersecurity.

What Is GDPR? It's More Challenging Than You Think

Today's computer systems are home to more and more data that affects the lives of global citizens. Medical records, personal data related to business transactions. And other such personally identifiable information may be stored among a network of global computer systems. Up to now there has been very little control over how such information is stored, managed, archived, or ultimately destroyed. In many cases our personal data is sold from company to company sometimes without our knowledge. This information can be used for good to provide us with better products and services but sometimes can also compromise individual privacy or be used for criminal purposes. Given the patchwork of global regulations that exist, the EU has sought to address this issue head on. GDPR is the most important change in data privacy regulations in a generation. In April 2016 the EU commission and the parliament adopted what is now known as the general data protection regulation ("GDPR"). GDPR was intended to replace the current patchwork of national data protection laws with a single set of rules directly enforceable in each EU member state. GDPR is designed to harmonize national data protection laws across the EU while at the same time modernizing the law to address new technological developments such as cloud computing, the Internet of Things (IoT), mobility, and many others.

GDPR is directly applicable and enforceable in all 28 EU member states as of May 25, 2018. Although not intended explicitly for validated systems, this law impacts privacy for both validated and non-validated computer systems. The principles of managing data under the new GDPR regulation are as follows:

- Processed Lawfully, Fairly and In A Transparent Manner
- Collected For Specified, Explicit And Legitimate Purposes And Not Further Processed Without

Consent If The Additional Processing Is Incompatible With The Original Purpose
- Adequate, Relevant and Limited To What Is Necessary
- Accurate And, Where Necessary, Kept Up To Date
- Kept In A Form Which Permits Identification Of Data Subjects For No Longer Than Is Necessary
- Processed In A Manner That Ensures Appropriate Security Of The Personal Data

At a very high level GDPR impacts people, processes and technology. Its basic premise is that today's computer systems must deliver privacy by design. In consideration of the three aspects addressed by GDPR, the following considerations must be addressed:

People

- Stakeholders
- Data Subjects
- Rights And Freedoms
- Lawful And Fair Processing
- The Right To Be Forgotten

Processes

- Data Access
- Data Processing
- Data Holdings
- Data Mapping
- Data Transfers
- Breach Response
- User Awareness And Training

Technology

- Security
- Data Storage
- Data Erasure/Deletion
- Data Archive And Retention
- Identity And Access Management

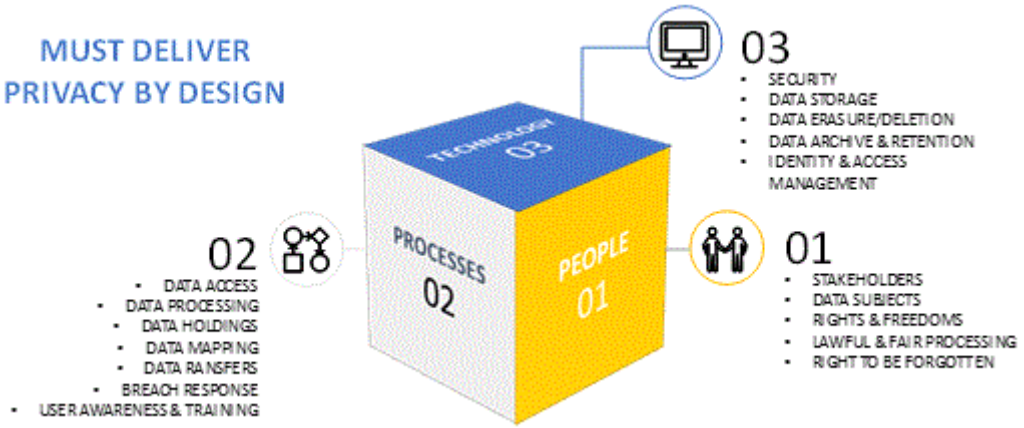

Figure 1 - People, Processes and Technology with GDPR

The ultimate success or failure of GDPR is predicated on how these three elements come together. Technology must deliver the ability to protect and defend personally identifiable information through its data storage erasure deletion archival and retention capabilities as well as identity and access management. Processes must ensure that data is protected throughout its entire life cycle and ultimately people must be not

only trained but held accountable for the management of data. Global citizens must be ever vigilant in terms of understanding how data is being managed and requesting the right to be forgotten if necessary.

There are primary requirements inherent in the new GDPR regulation. These requirements are as follows:

1. Data Breach Response
2. Privacy Engineering and Management
3. Investment In Human Resources
4. Increased Data Governance and Inventory
5. Management of Third-Party Information Systems
6. Data Erasure
7. Data Portability
8. Customer Transparency

Each one of these aspects may have a profound impact on an organization based on the extent to which they are implemented.

GDPR Impact Across Geographical Boundaries

In reading this paper you may be asking how does this apply to me if I am not managing systems or, the system may have its origins in the United States but may be implemented to support entities within the EU. GDPR applies to companies located in the EU and outside of the EU where processing activities related to goods and services are offered to EU nationals or where the behavior of individuals located in the EU is monitored regardless of whether the processing activities takes place within the EU or whether the individual is an EU citizen. Therefore you may have a system established and managed in the United States that includes supply chain data, clinical information, medical device information, or other such personally identifiable information that impacts EU citizens, you may be subject to the regulations defined in GDPR.

Thus, if GDPR affects these systems, how must we as validation engineers change our processes to ensure that these systems are tested in accordance with the new law.

What is “personal data”?

According to the definitions in article 2 of directive 95/46/EC,

“personal data” is any information relating to an identified or identifiable natural person (double quote data subject double quote); and identifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural, or society identity.”

Given this broad definition of personal data, think of your ERP, MRP, content management, clinical, LIMS, quality management system or other systems that you validate and the potential personal data held they are in. If you hold data for any EU subjects, those systems are not only subject to validation but they are subject to the regulations included within GDPR.

Controllers Versus Processors

GDPR distinguishes between two entities which are “Controllers” or “Processors”. A controller is any business that determines the purposes and means of processing personal data. For example this may be a life sciences company that collects personal data and any type of validated or enterprise computer systems such as an document management systems, MRP system, device design control system, cloud-based ERP systems, credit management databases, clinical trial systems, laboratory information management systems (LIMS), and many others.

On the other hand processors are any businesses that process personal information on behalf of the

controller. For many validated computer systems, this may be the cloud provider as the processor. Consider Microsoft dynamics 365 ERP system. This system resides in the Azure cloud environment. Therefore, Azure would be considered the processor under the responsibility of Microsoft.

Data processing is an old term which is not much used anymore but for the purpose of the GDPR regulation has been revived. Data processing is broad and covers everything organizations do with personal data including but not limited to:

- Obtaining and Collecting
- Maintaining
- Archival and Storage
- Duplication
- Backup and Recovery
- Encrypting and Decrypting
- Analyzing or Profiling
- Reading or Viewing
- Sharing or Disclosure
- Deleting or Destroying
- Transferring or transmitting (e.g. to a system even if the data remains in the UK)

GDPR requires the lawful processing and storage of personal data for subjects within the EU. The figure below illustrates the legal ground for processing personal data. To comply with the law, the following criteria must be adhered to:

1. Consent: an individual has given clear consent for you to process their personal data for a specific purpose
2. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
3. Legal Obligation: the processing is necessary for you to comply with the law (not including contractual obligations)
4. Vital Interests: the processing is necessary to protect someone’s life.
5. Public Task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
6. Legitimate Interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party (this cannot apply if you are a public authority processing data to perform your official tasks).

Figure 2 - Compliance with GDPR

Key Changes To Individual Rights

Under the new GDPR regulations, individuals have very specific rights concerning data processed on their behalf using personally identifiable information. Individuals have:

- The Right To Be Informed
- The Right Of Access (impacts computer systems validation)
- The Right To Rectification
- The Right To Erasure (impacts computer systems validation)
- The Right To Restrict Processing (impacts computer systems validation)
- The Right To Data Portability (impacts computer systems validation)
- The Right To Object
- Rights Related To Automated Decision-Making And Profiling (impacts computer systems validation)

When thinking about validated computer systems there are two aspects of the newfound rights that EU citizens have regarding personally identifiable information. EU citizens have the right to be forgotten in any computers system. Therefore as validation engineers we need to test that we have the right to forget an individual within a computer system without impacting the validated state of the system. As you well know in quality management systems deletion is typically not allowed. During system implementation we often test to ensure that data cannot be deleted specifically as it's related to quality transactions. GDPR however asked us to forget an EU citizen upon request.

This feature has huge implications on how data is tracked and managed within the system. This presumes that we have the ability to not only identify personally identifiable information but to remove it from the system without impacting other transactions. This is an element required by the regulation that may not have been thoroughly considered. One such instance for example is if an EU citizen signed a transaction and then requested the right to be forgotten. How with this right be implemented and how would we validate the system to ensure that we have the ability to be able to do as the regulation instructs.

Data Breaches in Validated Computer Systems

In today's computer systems environments, we are hearing more and more about data breaches affecting leading global companies as well as small companies. This is one aspect of computer systems where smaller companies and larger companies experience the same vulnerabilities. Although data hackers focus on target rich companies like global multinationals, small companies are equally as vulnerable to cyber-attacks.

In the new GDPR regulation, controllers must report breaches within 72 hours to the supervisory authority and affected data subjects at risk. Failure to report such data breaches may result in punitive fines of up to either 4% of group annual turnover or €20 million. The penalty for noncompliance with GDPR is steep as it should be. Recent breaches and cyber attacks by large multinational companies have gone unreported for unnecessarily extended periods of time. Companies have gotten away with not reporting data breaches or alerting the public that their data has been exposed thus leaving consumers vulnerable and subject to even greater attacks. Identity theft and the personal impact on consumers has been great. One would argue that much of the cost of such data breaches has been transferred by the individual citizen. One of the many goals of GDPR is to address this inequity. The lifecycle of personal data within an ERP system is used to illustrate this point as shown in the figure below.

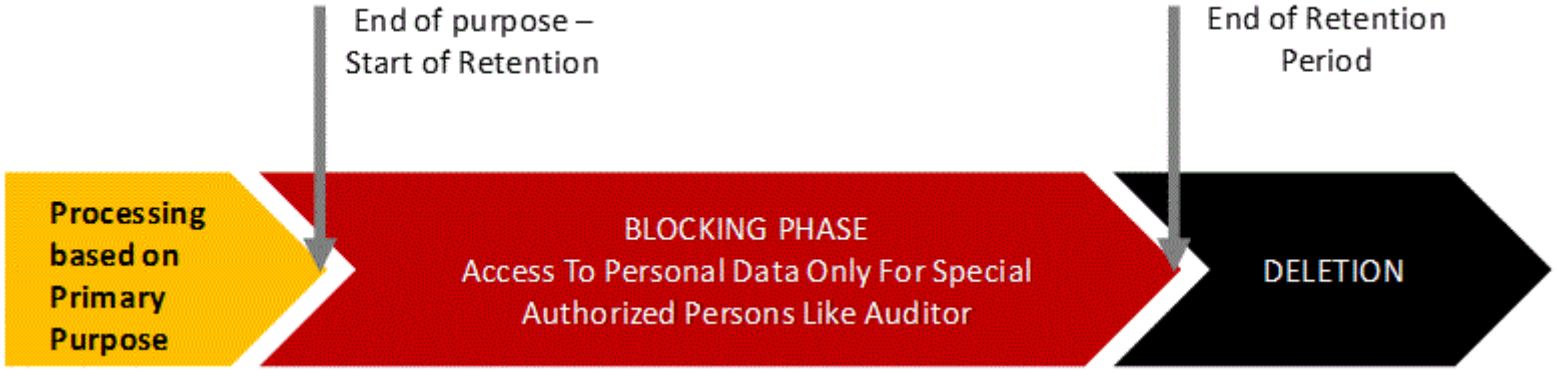

Figure 3 - Lifecycle of personal data in a sample ERP system

One of the core principles of GDPR is data should be retained in computer systems for as long as is necessary. Once data is at the end of its stated purpose, it should be deleted according to GDPR. As you can see from the illustration above the system goes through a primary purpose phase where the personally identifiable data is being used for its primary purpose. Once the primary purpose period is completed the data enters into what is known as a blocking phase where access to personal data is used in a very restricted manner such as for a special authorized person like an auditor for example. During the blocking phase period data may not be transferred or accessible by anyone outside of those who are authorized or given special access. Once the blocking phase comes to its conclusion, it signals the end of the retention period and the data must be deleted. Companies must have proof that the data has been deleted and erased from all corporate archives. Validation engineers must think of the implication of this as it relates to validation.

Time To Rethink Validation Strategies

Given the implications of the new GDPR regulations, validation engineers are forced to rethink how computer systems are tested and maintain going forward. There are some strategies that I believe are essential to ensure compliance with the new GDPR regulation. These new validation strategies are as follows:

- New Risk Assessment Strategy - validation risk assessments must now include GDPR related risk to ensure compliance. Computer systems may now be more vulnerable to cyber security risk, data exposure risk, and privacy risks. There is a significant business risk that may result in up to 4% of turnover in the event of a data breach. Each of these risk must be identified with mitigation strategies and control strategies to help either eliminate the risk or to minimize the risk as much as possible
- GDPR Response - companies must have the ability to respond to data breaches within 72 hours and report data breaches as per the new regulation. For new validated systems it is our recommendation that these technical controls be tested as part of the IQ/OQ/PQ and UAT testing strategy to ensure compliance. The validation team will be called upon to confirm that the system meets GDPR regulations.
- Documented Evidence For Validated Systems - as with all validated computer systems you must have documented evidence to support compliance with GDPR regulations. This documented evidence must be archived with each validation package.
- GDPR Impact - one of the first things validation teams should do is to identify whether or not your system is subject to GDPR impact. This is an important consideration and should be done as part of the validation determination process. When determining if a system is subject to 21 CFR part 11, GxP, and other predicate rule requirements, validation engineers should also assess the impact of GDPR and identify if any personally identifiable information is included within the validated computer system as well as the strategy for managing such data. If GDPR is impacted, clear testing strategies must be developed to ensure compliance.
- Deletion of Data - for validated computer system subject to GDPR validation engineers must be able to of data upon request. It is strongly recommended that standard operating procedures be developed that define the process for the deletion of data, formal response to data breaches, and the confirmation of data to be delivered to an EU citizen upon request
- Training - GDPR is unlike any other regulation in that “the right to be forgotten”, data deletion, and reporting requirements place a unique burden on IT organizations and validated computer systems. Thus, in preparation for the readiness to implement systems in accordance with GDPR it is very important that users be trained to understand the requirements of this regulation and what they mean with respect to computer systems.

Understanding GDPR & Computer Systems Validation - What You Need To Know

Most validation testing conducted today only touches the tip of the iceberg. Testing is basically functional in nature only testing features and functions within the software application for normal use. In today’s validated systems environment, testing of privacy controls, breech responses, and data erasure is paramount to compliance with GDPR. In addition to confirmation that a system meets its intended use, today’s systems in a GDPR environment must confirm that the system meets the technical requirements of this regulation. It is strongly recommended that a review of this regulation vis-à-vis current validation processes be conducted to ensure that procedures are sufficient to address the regulatory requirements of GDPR. Failure to do so could result and up to 4% of a company’s turnover.

For validated computer systems you need to think about the following:

- Does your validated systems support GDPR Reporting Requirements?
- In the event of a data breach, are your validated systems ready to respond?
- Have You Addressed “Right to be Forgotten” in Validated Systems?
- Does your risk assessment include GDPR risks?
- Is GDPR incorporated in your validation strategy?
- Do you have processes that require testing of GDPR technical controls?
- For you ERP and other validated systems, do you have consent policies in place to allow processing of personal data?

Questions for Validation Test Engineers To Ponder

1. Are your internal privacy controls robust and tested during validation?
2. Is the data you store portable and transferrable and tested during validation?
3. Can you completely erase personal data within your systems if it is no longer needed? What is the overall impact on your electronic records?
4. Can you quickly recognize and report a breach within 72 hours of the breach? Is this tested during validation?
5. Does your supplier audit process document 3rd parties compliance with GDPR?

To ensure compliance you need to have an affirmative response to each of these questions. One thing to consider and all of this is that although the regulation is an EU regulation many computer systems span across multiple geographical boundaries. The challenge of meeting GDPR may not be restricted to EU data processing systems therefore organizations need to understand the type of data housed within their systems and how to manage it. It is a good idea to have a cyber security strategy as well as a GDPR strategy in mind. One of the key recommendations out of all of this is to have standard operating procedures that provide governance for GDPR. It is important to train and understand this important legislation and what it means for your company. If you are multinational company that conducts computer systems validation across geographical boundaries you will clearly want to understand this regulation and the penalties associated for noncompliance. What the EU is saying with the new GDPR regulation is that it is no longer acceptable to have data breaches and wait years in some cases to report those data breaches. What they are also saying is privacy should be your guiding principle. Personally identifiable information should not be transferred from company to company without notifying the owner of that information so that they can understand the unique vulnerabilities of this information.

FINAL THOUGHTS

Personally identifiable information is being used against its owners to compromise their identity and wreak havoc and other ways. The EU has taken the first grand step to eliminate a patchwork of regulations to address this omnipresent risk associated with personally identifiable information. It is clear that as global regulators understand the impact of new computing systems environments they will change the way data is managed in their countries as well. This includes the United States.

The US has its own unique challenges associated with data breaches impacting personally identifiable information as has been highlighted by high profile breaches mentioned earlier. As medical device technology, pharmaceuticals, Biologics and other global entities become more and more automated the need for such a regulation is clear. How far other countries will go is an open debate. However what is not debatable is the need for readiness to protect global citizens and companies alike.

Global business systems fuel our economy and power the growth. Privacy is a key consideration and a very hot topic today. The take away for validation engineers is to become aware that we need to change and rethink our validation strategies to include today's reality. It is no longer acceptable to simply conduct IQ/OQ/PQ/UAT testing as we did in the 1980s. Technology has radically changed the way we live and work. Privacy is a reality. Success in today's digital realm depends on how well you manage and validate private information.

It's time that we rethink the way we validate today's technologies and move to 21st century approaches to validation which takes into account privacy, cybersecurity and compliance.

Tags:
GMP - Documentation & Records and Reports

Valarie King-Bailey
Valarie King-Bailey is the CEO of CEO of OnShore Technology Group, an independent Chicago-based consultancy specializing in Independent Validation and Verification (IV&V) products and solutions.

OnShore’s product,...
View Author Bio
