FAQ Sheet
EU General Data Protection Regulation

This document is intended to provide a broad review of the EU General Data Protection Regulation (GDPR) and is not intended to provide legal advice. STC urges ERI to seek guidance through its own legal counsel to understand how this new regulation defines its day to day operational requirements.

STC Consultants, LLC

Table of Contents

Executive Summary

The General Data Protection Regulation (GDPR) was ratified in mid-2016 and immediately became law. GDPR's purpose is to strengthen the protection of personal data to keep up with rapid technological developments, increased globalization, and more complex flows of personal data across borders. It is the most far-reaching global data protection law enacted to date in the European Union (EU) or elsewhere in the world. There was a 2-year implementation period, which expired on the 25th of May 2018. GDPR is now in full effect.

At its core, the 204-page directive raises the bar for privacy and data protection, with its inspiration coming from the Organization for the Economic Co-operation and Development (OECD) in the 1980's. This regulation enables individuals to better control their personal data by introducing a common set of rules that cross the European footprint. According to the European Commission, "personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address." [1]

These unified rules require businesses to build cohesive practices across the EU and create a single Digital Market. By doing so, it potentially reduces the cost of compliance with disparate and layered regulation and legal rulings across nations for companies. It also provides consumers a level of confidence that their private lives are kept private. Also, despite Brexit, this regulation will still be relevant to the UK, as the Data Protection Act 2018 has made requirements of the GDPR law in the UK.

While it applies to EU citizens, it is applicable for any organization with greater than 250 employees and that collects, manages and engages with European personal data, both inside and outside of Europe. As Computer Weekly states in its January 2016 web article, "this is really about the digital economy at its core and thus it will affect all businesses, not only in Europe. The final text of the GDPR incorporates the concept of "monitoring the behavior" of EU residents by tracking their digital activities. This is a very wide net given that most companies today do this as a key activity in conducting business. Computer Weekly calls this out by saying the final text in the GDPR really establishes that "This is as wide as it gets when it comes to the applicability of the GDPR, given that pretty much every website and app in the world does that".[2]

This is a truly complex piece of legislation that hopes to solve the primary concerns of people; safeguarding their privacy by introducing new requirements for companies in several key areas:

- Right to data access: EU citizens have the right to request and receive what data is collected and possesses has on each member, as well as where it is housed and in what way it is being used.
- Data portability: EU citizens can request that your company transmit their data to another business entity, thereby speeding up the user in switching services or providers
- Right to rectification: Right to change any incorrect information that a data controller has stored and has access to.
- Right to be forgotten: Citizens can provide direction to delete all information on them, "data erasure", and can also revoke consent from a company completely moving forward.
- Breach notification: For both Controllers and Processors, EU affected individuals must be notified within 72 hours of a data breach "without undue delay."

The ABC's of the GDPR

What Does it Regulate?

The GDPR regulates the "processing" of data for EU individuals, which includes collection, storage, transfer, or use. Any organization that processes personal data of EU individuals is within the scope of the law, regardless of whether the organization has a physical presence in the EU. Importantly, under the GDPR, the concept of "personal data" is very broad and covers any information relating to an identified or identifiable individual (also called a "data subject").

What sort of data will fall under the General Data Protection's Regulation? It will include but not be limited to the following items, and be aware that as the digital fingerprint extends so does the coverage of the regulation in this new digital world.

- Name,
- Photo,
- Identification number,
- location data,
- Email address,
- Social media posts,
- Personal medical information (including genetic and biometric data),
- IP addresses,
- Bank details, etc.

How Will Personal Data be Defined?

Personal data moving forward will be data regardless of it being private, public or work-related data that can singularly identify, directly or indirectly (either directly or by reference) "to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person" [3].

Thus, moving forward the sphere of personal data identifiers will also be extended to online data (routing IP address, location cookies and so forth) if this data can in any way be linked back to the citizen/subject.

Moving forward, "there is no distinction between personal data about individuals in their private, public or work roles - the person is the person".

Does the GDPR Affect My Organization? [4]

If you are processing personal data in the context of an organization established in the EU, the GDPR will apply to you, regardless of whether you are processing personal data in the EU or not.

"Processing" means any operation performed on personal data, such as collection, storage, transfer, dissemination or erasure.

If you are not established in the EU, the GDPR applies to you if you are offering goods or services (whether paid or free) to EU data subjects or monitoring the behavior of EU data subjects within the EU. Monitoring can be anything from putting cookies on a website to tracking the browsing behavior of data subjects to high tech surveillance activities.

Under European data protection law, organizations processing personal data are divided into "Controllers", or the entities which control the personal data, and "Processors", the entities that process personal data only on the instructions of the Controllers. The GDPR rules apply to both Controller and Processors.

How Will This Regulation be Managed - Model?

Answer: Through the roles of Controllers and Processors

Responsibility and its duties to implement the regulation is determined by the underlying role of those entities who control data and those who process the data.

The GDPR places emphasis on the obligations of data controllers (those who determine when, how and for what purpose personal data is to be processed). However, it also imposes a significant number of new requirements directly on data processors (those who process data on behalf of data controllers). Data processors now have a far greater requirement given they were previously subject to only to the contractual obligations imposed on them by data controllers. [5]

A new accountability principle will apply that will require companies that process EU personal data to create and maintain records demonstrating their compliance with the relevant GDPR requirements.[6] Moving forward, controllers are obligated to engage with only processors whom can provide sufficient guarantees to the technical process requirements, and who have the organizational command and controls in place to meet the new regulatory thresholds to protect the rights of the Subject's "identifiers". In effect, data controllers will be the overseers of the processors (to ensure they operate and meet the new regulatory requirements). While both will be held accountable to "implement appropriate technical and organizational measures" taking into account "the state of the art and the costs of implementation" and "the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals", the onus to comply is on the controllers of the data.

The new controller – processor relationship requires documentation and management through contracts that mandate the regulatory obligations to uphold data privacy. At the end of the day, it will the responsibilities of controllers to ensure the processor's privacy capabilities [7] meet the requirements of the regulation.

Types of Security Compliance?

The following suggestions come from the regulation and identify the type of security actions that would be considered "appropriate to the risk" compliance work effort. [8]

- The pseudonymization and/or encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of systems and services processing personal data.
- The ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Controllers and processors that adhere to either an approved code of conduct or an approved certification may use these tools to demonstrate compliance. Compliance and accountability will be with the controller – who must be sure of the processor's process model and privacy capabilities before handing off the first byte of critical data.

Means of Enforcement and Penalties?

Enforcement of the regulation will be driven via fines for those organizations noted in next section, both within the EU nations or Internationally operating within the EU, who do not comply. There are two tiers of violations:

1. Violations of record-keeping, security, breach notification, and privacy impact assessments can receive significant penalties, as regulators will now have the authority to imposed penalties up to the greater of $10M Euro or 2% of a company's global gross revenues.
2. Where violations occur in the areas of legal justification for processing (i.e. consent not provided), data subject rights, and cross-border data transfer violations, penalties can result in the greater of 20M Euro or 4% of global revenues (2x the financial ramifications).

How regulators will actually identify, target and enforce this new regulation once it goes into effect is yet to be seen – but they carry a potentially big stick. In the end, it will be as potent as those who can identify the violations and at what cycle times it takes to deliver swift compliance and heavy penalties.

Who will be the Enforcers? Do I need a DPO?

Regarding the regulation oversight teams of the GDPR, the following data was sourced directly from the europa.eu website. [9]

European Data Protection Supervisor
The regulation established a European data protection supervisor (EDPS) to uphold the rules governing the privacy rules set by the GDPR. It is responsible for monitoring the process and application of data protection rules within European Institutions and for

investigating complaints. Process oversight can include the collecting, recording, storing, retrieving, sending, blocking or erasing of data.

Snapshot of Department:

- Role: Ensures that EU institutions and bodies respect people's right to privacy when processing their personal data
- Supervisor: Giovanni Buttarelli
- Assistant Supervisor: Wojciech Wiewiórowski
- Location: Brussels (Belgium)
- Responsibilities:
    1. Supervises the EU administration's processing of personal data to ensure compliance with privacy rules
    2. Advises EU institutions and bodies on all aspects of personal data processing and related policies and legislation
    3. Handles complaints and conducts inquiries
    4. Works with the national authorities of EU countries to ensure consistency in data protection
    5. Monitors new technologies that might have an impact on data protection.
    6. For everyday operations, the EDPS comprises 2 main entities:
        - Supervision and Enforcement - evaluates data protection compliance by EU institutions and bodies.
        - Policy and Consultation - advises EU legislators on data protection issues in various policy areas and new legislative proposals.

Data Protection Officer in the European Commission

The European Commission has appointed a Data Protection Officer to be responsible for monitoring and applying the data protection rules in the European Commission.

- Role: The data protection officer independently ensures the internal application of data protection rules in cooperation with the European data protection supervisor."
- President: Jean-Claude Juncker
- Location: Brussels (Belgium)
- Responsibilities:
    1. Inform Commission departments collecting personal data ('controllers') and persons whose data are collected ('data subjects') of their rights and obligations under Regulation 45/2001
    2. Ensure Commission departments comply with the law when processing personal data
    3. Investigate data-protection matters
    4. Keep a register of processing operations on personal data by Commission departments
    5. Cooperate with the European Data Protection Supervisor

Does my business need to appoint a Data Protection Officer (DPO)?

DPOs must be appointed in the case of (a) public authorities, (b) organizations that engage in large-scale systematic monitoring, or (c) organizations that engage in the large-scale processing of sensitive personal data (Art. 37). If your organization doesn't fall into one of these categories, then you are not required to appoint a DPO.

Key GDPR Data Changes Implemented

The following section was sourced from the Sales Force.com white paper and outlines the chages of the data protection laws change moving forward. [10]

Expanded Definity of "Personal Data"

The GDPR expands and clarifies the concept of personal data. While the basic concept of personal data largely remains the same, the GDPR makes it clear that location data and online identifiers, such as IP addresses, are considered personal data. The GDPR also expands the concept of sensitive personal data to include genetic data and biometric data.

Expanded and new rights for EU individuals

The GDPR provides expanded rights for EU data subjects such as:

- Deletion: This right is sometimes referred to as the "right to be forgotten". The data subject has the right to require that the Controller erase personal data about him/her in certain conditions, including if the personal data is no longer necessary for the original purpose of the processing or if the data subject withdraws consent for the processing. This right has been extended to the online world as a means to require internet service providers to delete out-of-date publicly available information, in particular, that information which appears in search results.
- Restriction: Under the GDPR, a data subject has the right to obtain from a Controller a restriction on the processing of personal data in a number of circumstances, including if the accuracy of the personal data is contested by the data subject for a certain period of time. A restriction on processing means that the organization holding the data is entitled to continue to store it, but cannot process it any further.
- Portability of personal data: Data subjects also now have the right, in certain circumstances, to receive the personal data that they have provided to a Controller in a structured, commonly used and machine-readable format. Salesforce's data processing addendum takes into account these expanded and new rights.

Security Measures

The GDPR requires Controllers and Processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks presented. At Salesforce, we have robust security measures in place that meet the highest standards in the industry. For some of our services, we have security certifications including the International Organization for Standardization (ISO) 27001 and 27018 standard, the American Institute of CPAs' (AICPA) System and Organization Controls (SOC) reports, the Payment Card Industry Data Security Standards (PCI), the TÜV Rheinland Certified Cloud Service, TRUSTe Certified seal, and the UK Cyber

Essentials Scheme. For further details about our security measures in respect of specific services, please see our Trust and Compliance documentation.

Breach Notification

The GDPR requires organizations to report certain personal data breaches to the relevant data protection authority, and in some circumstances, to the affected data subjects. Controllers must notify the relevant data protection authority "without undue delay" (and where feasible, within 72 hours of having become aware of it), unless the breach is not likely to present any risk to the rights and freedoms of the data subjects concerned. If circumstances require it, Controllers may also be required to communicate the data breach to data subjects. Processors, for their part, are required to notify Controllers "without undue delay" after becoming aware of a personal data breach. Salesforce's data processing addendum takes into account this new obligation.

Data Protection Impact Assessments

Where certain processing is likely to be classified as "high risk" to data subjects, the Controller may be required to carry out a data protection impact assessment identifying the impact of the proposed processing operations on the personal data. Salesforce's data processing addendum takes into account this new obligation.

International Transfers

European data protection law restricts the transfer of personal data outside of the EU unless there are appropriate safeguards in place to protect that data. The GDPR continues to recognize current mechanisms (e.g. EU standard contractual clauses, EU Commission adequacy decisions, etc.) for legally transferring personal data outside of the EU. The GDPR also formally recognizes Binding Corporate Rules ("BCRs"), a set of company-specific, group-wide data protection policies approved by European data protection authorities to facilitate transfers of personal data from the EU to other countries. In November 2015, Salesforce became the first top 10 software company in the world to achieve approval for its Processor BCRs from the European data protection authorities.

Consent

Consent is subject to additional requirements under the GDPR. The GDPR defines consent as "any freely given, specific, informed and unambiguous indication of a data subject's wishes through a statement or clear affirmative action". The concept of consent is used throughout the GDPR to legitimize certain processing activities from a legal perspective.

Transparency

The GDPR requires that Controllers provide data subjects with information about their processing operations at the time when the personal data are collected. This information includes the identity and contact details of the Controller, the contact details of the data protection officer (if relevant),

the purposes and the legal bases for the processing of the personal data, the recipients of the data and a number of other fields to ensure that the personal data is being processed in a fair and transparent manner. In addition, Controllers are required to provide information to data subjects even in circumstances where the personal data has not been obtained directly from the data subject.

Profiling

The GDPR introduces the concept of "profiling" or any form of automated processing that uses personal data to evaluate personal aspects and in particular to analyze or predict aspects relating to an individual's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. Data subjects must be informed of the existence of profiling and any consequences of the profiling.

Enforcement

Fines for non-compliance under the GDPR can be substantial. Data protection authorities have a number of enforcement powers under the GDPR, including the ability to fine organizations up to €20 million or 4% of annual global turnover, whichever is higher. These are maximum fines and it remains to be seen how regulators will use their newly-acquired enforcement powers.

One Stop Shop

Under the GDPR, organizations that are established in more than one EU member state or are processing personal data affecting data subjects in more than one EU country will have greater clarity about their supervising data protection authority. Supervisory authority for the main European establishment of that organization will act as the lead authority. This authority will cooperate with the other supervisory authorities concerned in respect of cross-border data protection issues.

Implications

To start to understand how this impacts ERI, it is important to understand how ERI and its customers are classified, a controller or a processor? Where does ERI and its clients fall in this new biforcated world? The following table illlustrates the differences between the two, and what its role differences / implictions under the new regulation. An organization is considered a controller or a processor based on how you answer the examples in the table.

Table 1 - GDPR Roles: Example Decisions from ICO on Data Protection Act [11]

Data Controller	*Data Processor*
• Has decided to collect the personal data and has a legal basis for doing so; • Determines the type and content of personal data to collect; • What is the data to be used for; • Defining which demographics, targets, or individual's data will be collected about; • If data is to be disclosed and under what circumstances and to whom; • Who and when access or other individual rights apply to data; • What are the retention guidelines and when and how are amendments executed?	• How will personal data be stored? • What is the security surrounding the personal data; • How personal data will be moved/transferred between teams and organization. • The ways and means in data retrieval of personal data; • Defining the methods and procedures for retaining data within the retention profile. • The how and means of data storage and deletion.
These decisions that can only be taken by the data controller as part of its overall control of data processing operation.	Within the terms of the agreement with the controller, the processor's role is to use its specialized skills in deciding how to carry out activities on the data controller's behalf.

This table shows how a processor applies its technical knowledge but cannot take business guiding "how" and "why" decisions on personal data. These definitions are flexible and allow roles to be distributed amongst controllers. An example can be where upstream clients and solicitors are both data controllers in relation to this internal personal data, where each has their own data controller responsibilities for access and security of internal personal data.

This hybrid role also applies to data processors who will in many cases also be data controllers of its own personal data, and thus acts as a Controller for this data and its upstream clients/suppliers, however is an active processor for activities it conducts for others under contract. Determining if an organization is a data controller or data processor will be driven by its processing role and responsibilities.

The following are examples provided by the ICO of Processing Companies, as they conduct business work for others (but will be controllers for internal data); [12]

- Market research company
- Payment services
- Mail delivery services
- Solicitors
- Accountants
- IT services
- Cloud providers
- Statutory bodies.

The key to applying these rules is that an organization cannot be both a data controller and processor for the same data processing activity; it must be one or the other.

Based on the questions noted in the ICO table above, and based on our interpretation of GDPR, ERI is most likely not impacted by the regulation for its asset destruction operations unless the physical asset is identifiable to an individual. If an asset can and is identifiable to an individual, ERI will be positioned as a data processor for servicing an asset's end of life service eco-system. Several areas that come to mind regarding ERI guidance in the new EU GDPR world:

- Due to ERI's retention of employee data and its critical role in the destruction of hardware with personal data stored on the drives, it should highly consider establishing a Data Protection Officer role to establish systematic reviews and governance oversight. This person will be required to have "expert knowledge of data protection law and practices.".
- ERI should conduct a full Data Protection Impact Assessment (DPIA). An article by Medium Corporation about GDPR Controllers and Processors identified the following factors when conducting a DPIA [13]
  1. A systematic process of processing.
  2. The purpose of the processing.
  3. Assess the purpose and the process of processing.
  4. Assess the risk related to individual's right to freedom.
  5. Measures to mitigate possible risk.

- Overall, enforcement action is squarely placed on the controller's shoulders. ERI should place itself in the controller's seat and validate the necessary measures are in place to remove vulnerability that may arise from your downstream data processors with employee's data.
- When a data controller provides personal data to another data controller, the second controller takes on the responsibility for any compliance failure on its behalf. This may be the case in numerous scenarios. Due to this assignment of liability under the new regulation, ERI should ensure processes are in place to care for and report out on this area of responsibility.
- Due to ERI's potential hybrid role, ERI should audit procedures in place for events where personal data are transferred to ERI overseas locations.
- For all outsourced data processors working on ERI's behalf, put in place:

    - Technical and organizational security measures governing the processing to be carried out, and
    - Establish regular audit plans to ensure compliance with those measures.
- Ensure there are written agreements with outsourced vendors in place for each area of compliance.
- As a potential data processor, ERI may be directly served with a warrant requiring it to provide certain personal data. This may move ERI to a controller role in its effort to comply with the enforcement agency's request. This exposes ERI to enforcement action if the response to such a request is not correctly executed. To remove some of this risk, ERI should validate compliance through requests of its supply chain/downstream partners;
    - Request the contracted data processor provide GDPR proof of compliance (allowing ERI to manage GDPR requests moving forward)
    - Request processor to manage the response to requests so ERI knows the partner can manage requests on ERI's behalf.

Source Material

1 European Commission's press release announcing the proposed comprehensive reform of data protection rules. (2012, 25 January), Retrieved 29 May 2018.

2 Ashford, Warwick (2016, 11 January), Computerweekly.com, "EU data protection rules affect everyone, say legal experts": https://www.computerweekly.com/news/4500270456/EU-data-protection-rules-affect-everyone-say-legal-experts

3 Galdies, Peter (2017, 12 October), Data IQ ", A summary of the EU General Data Protection Regulation": https://www.dataiq.co.uk/blog/summary-eu-general-data-protection-regulation

4 Salesforce.com – "White Paper: GDPR Key Facts" https://www.salesforce.com/content/dam/web/en_us/www/documents/white-papers/gpdr-fact-sheet.pdf

5 Squirepattonboggs.com – "GDPR-Implications": https://media.squirepattonboggs.com/pdf/misc/GDPR-Implications.pdf

6 Squirepattonboggs.com – "GDPR-Implications": https://media.squirepattonboggs.com/pdf/misc/GDPR-Implications.pdf

7 Galdies, Peter (2017, 12 October), Data IQ ", A summary of the EU General Data Protection Regulation": https://www.dataiq.co.uk/blog/summary-eu-general-data-protection-regulation

8 Galdies, Peter (2017, 12 October), Data IQ ", A summary of the EU General Data Protection Regulation": https://www.dataiq.co.uk/blog/summary-eu-general-data-protection-regulation

9 European Commission, "Data protection in the EU", **https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en**

10 Salesforce.com – "White Paper: FDPR Key Facts" https://www.salesforce.com/content/dam/web/en_us/www/documents/white-papers/gpdr-fact-sheet.pdf

11 Information Commissioner's Office (2014, 6 May), "Data controllers and data processors: what the difference is and what the governance implications are", https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

12 Information Commissioner's Office (2014, 6 May), "Data controllers and data processors: what the difference is and what the governance implications are", https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

13 Medium.com (2017, 12 September), "All you need to Know about DGPR Controllers and Processors", https://medium.com/@sagarag/all-you-need-to-know-about-gdpr-controllers-and-processors-248200ef4126