FAQ
General Data Protection Regulation

- Do I have to have a breach to be fined under the GDPR?
    - **Answer:** No, simply being non-compliant with the regular puts you at risk of being fined by a member state supervisory authority (SA).

- My company chose to host in the E.U (to avoid the U.S govt surveillance/Patriot Act), do we have to comply with the GDPR?
    - **Answer:** Yes, if you are hosting/processing data in the EU this would meet the establishment test and your processing would have to be compliant if you are processing personal data. (You should seek the guidance of a counsel on the risk.

- My organization is based in the U.S but we sell goods in the E.U – do we fall under the scope of the GDPR?
    - **Answer:** Yes, if you sell goods to EU residents, most likely your org. would fall under the scope of the GDPR**.**

- We use Microsoft Office 365 hosted in the E.U, does that fall under the scope of the GDPR?
    - **Answer:** Yes. Office365 often contains personal data (email addresses, IPs, other data elements) that would fall under the scope of the GDPR.

- With the uncertainty around the legality of the Standard Contractual Clauses, what is the best way to transfer data legally?
    - **Answer**: The standard contractual clauses are still a valid legal mechanism for cross-border data transfers. You may want to consider other vehicles as well; EU-US Privacy Shield, or Binding Corporate Rules (BCRs).

- What exactly is a joint controller? Where does the liability lie in this relationship?
    - **Answer:** A joint controller is essentially a situation where 2 (or more) entities or organizations are making the decisions around the processing of personal data.

    - Both controllers would have statutory obligations under the regulation. Liability would need to be defined within the scope of the relationship.

- Will my cyber coverage cover non-compliance issues with the regulation?
    - **Answer:** Cyber coverage can cover regulatory non-compliance violations where it is not precluded by law.

FAQ
General Data Protection Regulation

- Is there a grace period to become compliant after May 2018?
    - **Answer:** No. The law goes into force on 25, May 2018. The grace period (essentially) was from when the regulation was passed in 2016 until 2018 when it goes into effect.

- What does GDPR consider to be protected data? Do business email addresses really fall under scope? IP addresses? MAC addresses? Documents?

    - **Answer**: There is a very broad definition of personal data under the GDPR. Personal data is defined as identified or identifiable (directly or indirectly) data that can be used to identify a natural living person in the EU. Some of these elements include: Name, address, phone numbers, IP addresses, email addresses (including business), MAC addresses, biometrics, trade union membership, etc…. When reviewing what type of data that you have, you need to be very diligent and potentially cast a wide net to catch all of the potential personal data in your org.

- What will the enforcement environment be like?
    I. Germany: sent letters to 500 companies (mostly U.S businesses) asking them to demonstrate compliance

    II. CNIL: very active enforcement arm- hires college interns to troll the web for companies offering services in France and review for ecookie, privacy notice, etc…

    - **Answer**: The message being put forth by the Supervisory Authorities is that they will be actively enforcing the regulation.

- Do we have to respond to Data Subject access requests from employees?
    - **Answer:** Yes. Employees personal data falls under the scope of the GDPR>

- Does the data we that collected before the GDPR went into effect fall under the regulation?
    - **Answer:** Yes. The regulation covers all personal data (of natural living citizens) regardless of when it was collected/processed.

- I have heard that if we are not established in the EU that we have to designate a rep. in the EU- is this true?
    - **Answer:** Yes. If you collect/process data of EU data subjects, you will need to designate in writing a representative in the EU.

FAQ
General Data Protection Regulation

- Do we have to update our contracts with vendors?
    I. We host in a data center, do we need to update those contracts as well?
    - **Answer:** All contracts should be reviewed to ensure compliance with the GDPR.

- What is the definition of a data breach under GDRP?
    - **Answer**: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed

- Is the GDPR really enforceable against non-EU companies?
    - **Answer**: Yes. Many countries have agreements in place to support trade, law enforcement, and other types of activities. In the U.S, the FTC has indicated that they will help enforce violations. In fact, the FTC just recently issues consent decrees against 3 U.S companies for claiming EU to US Privacy Shield certification when in fact they did not have the certification.