You are working for a company that has, to date, only operated in the United States.  You have just been told that the company is now purchasing an enterprise in England.  Discuss your strategy on bringing your U.S. unit in compliance with the provisions under the GDPR.  This may be a technology issue as well as a policy point.

The General Data Protection Regulation (GDPR) comes with a set of rules and regulations for the protection of personal data inside and outside the European Union (EU). It affects all companies that save personal data from European citizens. In order to be GDPR compliant, some of the steps that the company should take include:

* Understanding the different terms such as data subject, the data controller, personal data, and data processor.
* Auditing the company’s processes regarding the collection, storage, disclosure, and processing of data. An audit should be required before implementing any changes in the company since it gives an overview of what the organization currently has and may reveal incompatibilities that existing procedures may have with the GDPR.
* Creating and implementing an action plan that highlights where the company stands with GDPR, provides solutions for obstacles against compliance and makes a plan on how to execute them. The plan should also include a timeline and the identities of people or teams that would lead to the realization of the plan. For example, the GDPR will require some organizations to designate a Data Protection Officer (DPO). Organizations requiring DPOs include public authorities, organizations whose activities involve the regular and systematic monitoring of data subjects on a large scale, or organizations that process what is currently known as “sensitive personal data” on a large scale.
* Data protection impact assessments (DPIAs), as part of an action plan, are crucial for GDPR compliance. In fact, The GDPR introduces mandatory DPIAs for organizations involved in high-risk processing, such as new technologies being deployed, a profiling operation likely to affect individuals significantly, large-scale monitoring of a publicly accessible area, etc.
* Reviewing current policies as part of an action plan is also crucial for GDPR compliance. Once the company knows where its sensitive data resides, it should examine how its data and policies shape up to GDPR standards. Hence, the organization must create a list of policies and practices that meet GDPR standards and identify processes that could meet standards with slight modifications, including which areas need a complete overhaul.
* Taking to the legal team of the company. That is, GDPR is a set of regulations and imposes fines on people and firms that violate its rules. Hence, the company needs to consult its lawyers to know if the firm has any legal vulnerabilities or if there will be instances where the company may be compromised. The company must also draft procedures for handling such cases.
* Raising awareness and making sure the entire company is in the loop about GDPR and what the firm will do about it is critical for compliance. That is, GDPR is likely to cause sweeping changes across the organization. Hence, the company needs to prepare its employees for these impending reforms in the organization. That way, everyone will cooperate, and the company will smoothly transition to the post-GDPR operations.

All in all, it will be easier to decide which method best fits the company if the organization knows what steps it needs to take. However, this process will vary for each business, depending on how compliant the company already is. Some companies will only have to tweak a few procedures, while others will have to build compliance from the ground up.

References

<https://www.pacificdataintegrators.com/insights/Your-Step-by-Step-Guide-to-Becoming-GDPR-Compliant>

<https://www.codeinwp.com/blog/gdpr-compliance/>