**What is GDPR?** General Data Protection Regulation. Replaces local EU Data Protection Directive implementations (e.g., in UK the “Data Protection Act”). Starts on May 25, 2018

**Who is Subject?** All organizations that collect and process personal data of EU data subjects – regardless of size. No longer applies only to organizations with an office the EU - is borderless and it applies to data processors, not just data controllers

**What are the Penalties?** Up to 20M € or 4% of organization’s annual global turnover, whichever is higher (board attention is now guaranteed). Data subjects can claim compensation for damages from breaches to their personal data

**Main Areas of Focus for CareerViet for May 25, 2018**

- **Breach Notification** -Report Privacy breaches to the EU regulator within 72 hours and potentially to the data subject. On target to have compliant process in place by 5-1-18

- **Vendor Risk** -Evaluate vendor contracts and controls for adequacy to protect data subject data. Progressing. Formal Vendor Risk program under development. Key vendors have been identified and Data Processing Addendums being created for vendors.

- **Consent** -Requirement to gain unambiguous consent (i.e. explicit). Progressing with assistance from Protiviti/ Robert Half Legal.

- **Privacy By Design & By Default** -Updating existing SDLC and system procedures and policies to incorporate privacy and security into normal processes. On target to be in place by 5-1-18. SDLC processes being updated to include privacy and security in all system and application development processes.

- **Data Protection Officer (DPO)** -DPO required for organizations that conduct regular and systematic monitoring of data subjects on a large scale or process Special Categories of data (e.g., healthcare) on a large scale. On target to be in place by 5-25-18. Internal determination as to appropriate person and reporting structure in process.

- **Data Security** -Requirements to secure systems and data with best practice security programs. On target to be in place by 5-25-18. Evaluation of GDPR relevant security controls currently underway.

- **Data Subject’s Rights** -Develop ability to accept requests and respond for “the right to know”, “right of erasure” (“right to be forgotten”) and the “right to data portability”. Progressing. Portal to accept requests will be in place by 5- 1-18. A short-term process to (manually) respond to requests is being developed. Parallel effort to develop long- term automated process being developed.

- **Legal Basis for Processing** - Legal Basis for all processing activities being determined. On target to be in place by 5-1-18. All processing activities are being evaluated to determine appropriate lawful basis.

- **Records of Processing Activity** -All details of processing activities documented. Target to be completed by 5-1-18.

Protiviti are providing GDPR subject matter expertise services. They have conducted data discovery, mapping, and data inventories as well as the Records of Processing Activities. In addition, they are performing a GDPR Readiness Assessment to determine CareerViet’s gaps to reaching compliance. In addition, are providing valuable guidance and advice as CareerViet continue efforts towards GDPR compliance.

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Their consulting solutions span critical business problems in technology, business process, analytics, risk, compliance, transactions, and internal audit.