TIPS FOR AUDITING GDPR

Many auditors will be called upon to audit their enterprise's practices and controls to ensure compliance with the Global Data Protection Regulation (GDPR). The following checklist highlights some of the aspects an auditor should do as part of a GDPR audit engagement:

- **Review the process** undertaken by the business to locate and cleanse the data.
- **Assess the processes** and associated rules that have been established to validate the data collected.
- **Review the rules** that are put in place to minimize the instance of shadow IT systems and manage unstructured data.
- **Assess data quality annually** (at a minimum). Traditionally, data quality audits have focused on corporate data; with GDPR, these audits now need to cover personal data.
- **Validate that the systems created to ensure that personal data that have been put out of reach** as a result of a subject access request (SAR) keep those data out of reach in the event of a full restore from backup.
- **Consider whether the information provided is concise, complete, accurate and easily understandable.** If this is not the case, then the organization should look at the reasons why and amend accordingly.
- **To validate the "purpose" requirement of GDPR, create a schedule of uses of personal data and link this schedule to the personal data stored.** Auditors should expect that records are flagged with a reference to a defined purpose that will in turn define the basis. Auditors should also expect to see evidence of validation and a link to a records retention and deletion policy.
- **Validate storage processes and their consistent application.** Auditors should approach with caution and consider retention first and foremost in terms of other legislation and regulation before GDPR and the enterprise's needs. GDPR only replaces existing data protection legislation and does not overwrite other existing legislation such as that relating to record retention (e.g., for tax purposes).
- **Where electronic data recording systems are used and offer facilities allowing retention periods to be set, confirm that the facilities are being used and the configured retention dates conform to the policy's data review requirements.** In addition, it is incumbent on the auditor to assess whether the procedures are followed and are effective. Is the actual destruction of personal data properly carried out in accordance with the enterprise's policy? Does the enterprise dispose of IT software and hardware in a manner that fully conforms to the enterprise's policy?
- **Provide assurance** whether that the contracts register is maintained, complete and up to date and contains a robust approach to additions and deletions.
- **Determine whether a supplier risk assessment has been completed that serves to rank each supplier in terms of data risk.** If there is any doubt, the auditor should select a sample and ask the vendor to complete a GDPR compliance and data security questionnaire.

For more information on auditing GDPR, as well as a wealth of resources for both audit and privacy professionals, go to **www.isaca.org/how-to-audit-GDPR.**

© 2018 ISACA. All Rights Reserved.

ISACA®