BDO'S GDPR CHECKLIST

The General Data Protection Regulation (GDPR) is far-reaching. With steep penalties for organizations that are not in compliance, ensure that your organisation is taking the proper precautions to protect your data.

RELEVANCE & RESPONSIBILITIES

- [ ] Identify relevant business processes, systems and data sets likely to contain personal data.
- [ ] Determine whether your company processes personal data belonging to EU "data subjects".
- [ ] Determine your responsibilities as a data "controller" or data "processor"— or in some cases, both.
- [ ] Identify third parties who have access to or process the personal data you obtain.

READINESS

- [ ] Review your current data privacy and security policies against all relevant Authority Documents — not just GDPR — to identify synergies and gaps.
- [ ] Conduct a data mapping exercise to identify, classify and inventory all data assets.
- [ ] Review your contracts with relevant third parties to ensure you include GDPR-relevant language.
- [ ] Review privacy notices to ensure transparency, fairness and accessibility.
- [ ] Provide GDPR training to your staff.
- [ ] Test your incident response capabilities to ensure compliance with the 72-hour breach notification requirement.

REMEDIATE

- [ ] Develop a detailed remediation roadmap to prioritize and ensure timely compliance.
- [ ] Update policies and procedures or create new ones to address gaps.
- [ ] Implement privacy by design and privacy by default principles and security controls in all systems and processes.
- [ ] Review and update cross-border data transfer processes to conform with country specific conditions.

PREPARE FOR AUDIT

- [ ] Develop and maintain a data register to record all processing activities.*
- [ ] Designate and register a Data Protection Officer to serve as liaison to the relevant Supervisory Authorities.
- [ ] Document all ongoing policies, procedures and controls needed to substantiate compliance with GDPR requirements.
- [ ] Ask vendors to provide evidence they are taking steps to be GDPR compliant and conduct regular due diligence.

*Exemptions may apply to organizations with less than 250 employees

For more information on GDPR and protecting your organization's data, visit www.bdo.com.mt