CompliancePoint®

GDPR CHECKLIST

A guide to helping your organization measure its compliance posture with the European General Data Protection Regulation (GDPR)

- ☐ Appoint a Privacy Task Force comprised of individuals from at least the Legal, Information Technology and Information Security, Marketing, and Human Resources departments
- ☐ Determine scope of personal data through a Data Inventory exercise
- ☐ Determine where and how personal data flows and any sharing activities through a Data Mapping exercise
- ☐ Develop a Record of Processing based on Data Inventory and Data Map results
  - Include the lawful basis for each processing activity
- ☐ Determine if Data Protection Officer/EU Representative requirements apply and appoint if necessary
- ☐ Update the online privacy policy and employee policies to include Article 13 & 14 disclosure requirements
- ☐ Establish policies and procedures to honor data subject access requests under Articles 15-22 (Right to Access, Right to Rectification, Right to Erasure, Right to Restriction, Right to Data Portability, Right to Object, Right to Object to Automated Decision-Making)

- Verify the data subject's identity, apply exemptions, define "delete," establish a method to securely provide the personal data, and develop responses

- ☐ Review processing based on consent to ensure it is freely given, specific, informed and unambiguous and includes notice of the right to revoke consent
  - Update consent revision process to include a review for these requirements and ensure records are retained that include date/time stamp of all consent

- ☐ Assess and update security controls to comply with Article 32 Security of Processing requirements

- ☐ Establish policies and procedures to comply with the privacy principles (Lawfulness, Fairness, and Transparency, Purpose Limitation, Data Minimization, Accuracy, Storage Limitation, Integrity and Confidentiality, and Accountability)
  - Review retention policies and audit for compliance

- ☐ Update Incident Response Plan to include notification of data breaches to the Supervisory Authority and data subjects when required

- ☐ Establish policies and procedures to comply with the privacy by design/ default requirements

- ☐ Update vendor onboarding process to include a review for Article 28 processor obligations

- ☐ Determine if any personal data is transferred outside of the EEA and, if so, the approved mechanism(s) that will be relied on for the transfer

- ☐ Train employees on your organization's obligations under the GDPR on at least an annual basis

- ☐ Demonstrate compliance with Article 5 (2) Accountability Principle by establishing a monitoring and enforcement program surrounding GDPR compliance