PREPARING FOR GDPR

A COMPREHENSIVE CHECKLIST FOR COMPLIANCE

GDPR applies to any organization worldwide that possesses or processes European Union citizen data.

PLAN

☐ DETERMINE IF YOU ARE COVERED UNDER GDPR

Are you under 250 personnel or solely invested in national security concerns? If you answered yes to either GDPR does not apply.

☐ DETERMINE WHICH SUPERVISORY AUTHORITY IS THE RIGHT ONE

This aligns with how your organization looks to implement governance and controls around Personally Identifiable Information (PII).

☐ DEVELOP GDPR GOVERNANCE/MANAGEMENT PROGRAM

Technology, processes to budget, as well as supervisor agent reporting and board reporting.

Develop and maintain a Privacy Program that contains documented procedural and technical controls, alignment with existing security controls, data retention guidelines per PII type, and Program Continuous Monitor processes and guidelines.

Identify if the type of information or the method of collecting information warrants a Privacy Impact Assessment (PIA).

If a PIA is warranted:

- Provide detailed systems and process documentation on how the information is processed and stored.
- Develop method to interact with affected persons to collect information on the value versus the risk of collecting PII.

PII data exchanges have guidelines for technology, shared accountability, and shared liability.

Know which member state regulations and exemptions apply (National Security/Law Enforcement designated information).

☐ IDENTIFY A DATA PROTECTION OFFICER (DPO)

Amount of PII, how PII is collected, how PII is used, and business size are limiting factors to the number of duties a DPO can take on.

DPO contact information must be published and possessed by the supervisory authority.

☐ IDENTIFY SUBORDINATE DPOs

Ensure path of communications and reporting is consistent to support auditability.

Non-primary supervisory agents must have published contact information for DPO and associated subordinate DPOs.

☐ BUILD PLAN FOR DEALING WITH MULTIPLE TERRITORIES

Coordinate how information will be shared between DPOs and subordinate DPOs. Identify other applicable member state regulations.

☐ IDENTIFY LEGAL COUNSEL TO SUPPORT GDPR ASSETS

Put an emphasis on risk reduction versus pure compliance. GDPR is a risk reduction exercise similar to information assurance.

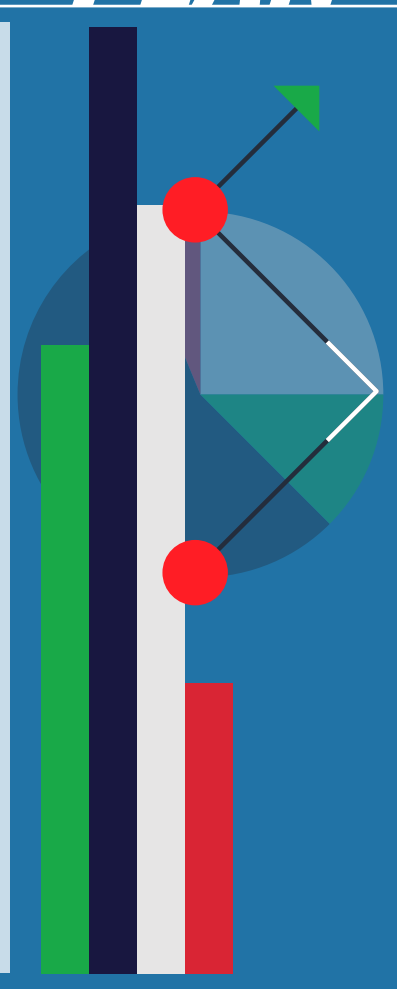
☐ DEVELOP A GDPR TRAINING PROGRAM

GDPR is about establishing a system of privacy protections for individuals. Account for people and processes, not just technology.

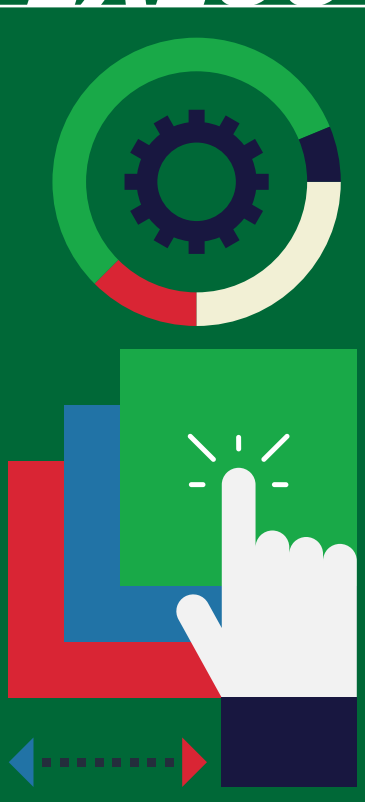
☐ IDENTIFY PROCESSORS

Determine responsibility for services:

- Liability in regards to PII.
- Sharing PII in an extra-group agreement.
- Removal of PII.



EXECUTE



☐ IMPLEMENT PSEUDONYMIZATION FOR PII (PRIVACY BY DESIGN)

Use technology to encrypt, hash, or tokenize information associated with PII. Encryption-based controls must trace at a minimum privilege and organizational policy for data retention.

Controls for pseudonymization must have controls for data exchange with other organizations.

Provide technology that can:

- Audit and log information
- Remove PII per valid request
- Provide log correlation to PII creation, retention, and removal

Provide capabilities for data subject transparency and access need traceability for personal data export.

Provide security controls, such as digital signature or hashing functions, to mark protested data and demonstrate that no alterations occur during the protest.

Seek fine-grained access controls that can make authorization to data utilization.

Provide controls for data exchange that expose only information required by the outside entity.

☐ EXECUTE PRIVACY IMPACT ASSESSMENT

Assess the reasoning for PII collection, assess the value of collected PII versus the risks of not having it with affected persons.

Have artifacts available when referring to a supervisory authority (high risk).

Demonstrate alignment between data breach response and PIA.

☐ IMPLEMENT & DOCUMENT TECHNOLOGY TO SHOW CONSENT / COMPLIANCE

Safeguards for minors (13 in the UK and Ireland, 16 in most of the EU).

Compliance with Web Content Accessibility Guidelines 2.0, level AA and consider tools that demonstrate non-repudiation, such as issued tokens, certificates.

Provide consent for cookies (or refrain from cookies), justify the collection of PII to customers, and maintain records that show consent for PII use.

Implement solutions such as SIEM or other platforms with audit reduction based on provenance and disposition of PII.

Implement solutions such as DLP and encryption services to protect PII that can tie directly into the broader GDPR audit enterprise.

Implement protections for whistleblowers and other irregular business activities.

MONITOR

☐ PROVIDE CONTINUOUS MONITORING OF TECHNICAL CONTROLS & PROCESSES

Develop audit views that show states of data sharing/transfer assets, and protest status/outcomes. Develop integrated auditing views of systems security with PII controls.

☐ AUDIT PIA OPERATIONS AND OUTCOMES

Provide documentation for PIA efforts and actions.

Be able to justify action/inaction based on PIA results.

☐ MAINTAIN COMMUNICATIONS COMPLIANCE WITH SUPERVISORY AUTHORITIES

Provide documentation that shows requisite communications with supervisory authorities and reporting as part of data breach response activities.

ENFORCEMENT DATE → 5.25.2018

Fornetix helps organizations unleash the full potential of encryption by conquering the key management bottleneck. Our Key Orchestration ecosystem automates the key lifecycle across the entire enterprise with groundbreaking precision and speed. For more information on how our products can help you meet GDPR compliance needs visit: www.fornetix.com

FORNETIX®