ManageEngine

A quick guide to Organic Law 3/2018 (LOPDGDD)

Organic Law 3/2018 (LOPDGDD), enforced by the Agencia Española de Protección de Datos (AEPD), adapts and supplements the GDPR for Spain. It governs how organizations process personal data and guarantees a set of digital rights.

Technical controls checklist

Use the checklist below to assess your organization's readiness across LOPDGDD's key requirement areas.

Sl.no	Requirement area	Article	Controls required
1	Data accuracy and integrity	Article 4	• Audit create, modify, delete actions on data • Alert on unauthorized change • Track data source and lineage • Rectify and erase without delay
2	Confidentiality and access control	Article 5	• Restrict access by role • Scope delegation by OU or group • Enforce adaptive MFA at login • Recertify entitlements periodically
3	Special-category data protection	Article 9	• Discover and classify sensitive data • Monitor file integrity • Prevent data exfiltration • Limit access to authorized roles
4	Data subject rights	Articles 11–18	• Locate an individual's data • Act on access and erasure requests • Report on identities and permissions • Document the action taken
5	Accountability and risk management	Article 28	• Adopt risk-based measures • Scan for misconfigurations • Enforce password policy • Back up and restore directory data
6	Records of processing activities	Article 31	• Record workflow and admin actions • Log access and permission changes • Retain activity centrally • Generate audit-ready reports
7	Processor and outsourced oversight	Articles 30, 33	• Collect logs from cloud and hosted systems • Monitor processor access • Alert on anomalous activity • Retain oversight of outsourced data
8	Breach detection and notification	Articles 28; DA 9ª	• Detect breaches in real time • Reconstruct scope and cause • Notify the AEPD within 72 hours • Document remedial action

LOPDGDD and ManageEngine

ManageEngine offers solutions that will help your organization govern access, monitor activity, and detect and respond to incidents affecting personal data. AD360, ManageEngine's IAM solution, covers the identity and access controls the law requires, while Log360, its SIEM solution, covers logging, threat detection, and breach handling. Used together, they help you implement the technical controls required under LOPDGDD.

How can ManageEngine help you implement LOPDGDD?

Role-based access governance

Restrict access to personal data by role, and scope delegation by OU, group, or attribute.

Helps with Article 5.

MFA

Enforce adaptive MFA across endpoints, VPN, and applications to protect data access.

Helps with Article 5.

Access certification

Recertify entitlements periodically so only authorized identities reach personal data.

Helps with Article 5.

Forensic investigation

Reconstruct who accessed personal data, when, and what changed for AEPD investigations.

Helps with Article 53 bis.

File integrity monitoring

Detect unauthorized modification, deletion, or corruption of files holding personal data.

Helps with Article 4.

Data loss prevention

Monitor and block exfiltration of personal data to guard confidentiality.

Helps with Article 9.

Record of processing activities

Record admin actions and access changes, and retain activity centrally for the processing register.

Helps with Article 31.

Cloud and processor monitoring

Collect and analyze logs from hosted and cloud systems to oversee outsourced processing.

Helps with Articles 30, 33.

Breach detection and response

Detect breaches with correlation and UEBA, then reconstruct scope and record remediation.

Helps with Articles 28; DA 9ª.

For more information, contact sales@manageengine.com