The Beginner's Guide to GDPR Compliance with Kitecyber

Discover how Kitecyber helps your organisation comply with the General Data Protection Regulation (GDPR) by securing personal data (PD) across endpoints, cloud, networks, and SaaS applications — preventing unauthorized access, loss, or misuse.

What is GDPR?

The General Data Protection Regulation (GDPR) is a European Union regulation enacted in 2018 to protect personal data and privacy. GDPR applies to any organisation processing personal data of EU residents, regardless of where the organisation is located.

GDPR mandates organisations to:

- Protect personal data (PD/PII) through technical and organisational safeguards.
- Ensure transparency and accountability in processing.
- Provide rights to data subjects including access, correction, and deletion.
- Report personal data breaches to regulators within 72 hours.

Who Must Comply With GDPR?

Data Controllers
Determine the purpose and means of data processing.

Data Processors
Process personal data on behalf of controllers.

Sub-processors
Vendors or cloud services handling personal data.

Non-compliance may lead to fines of up to €20 million or 4% of global annual revenue, whichever is higher.

Key GDPR Requirements

- **Lawful, fair, and transparent processing** - Process data with consent or legitimate grounds.
- **Purpose limitation** – Use data only for the specified purpose.
- **Data minimisation** – Collect only necessary personal data.
- **Accuracy** – Keep personal data accurate and up-to-date.
- **Storage limitation** – Retain personal data only as long as necessary.
- **Integrity and confidentiality** - Secure personal data against loss, theft, or unauthorised access.
- **Accountability & governance** – Demonstrate compliance with GDPR policies and procedures.
- **Data subject rights** – Support access, correction, erasure, portability, and objection requests.
- **Breach notification** – Report personal data breaches within 72 hours.
- **Privacy by design & by default** – Integrate privacy in systems and processes from the outset.

info@kitecyber.com
www.kitecyber.com
KITE CYBER

How Kitecyber Helps Organisations Comply with GDPR

Kitecyber unifies **DLP, UEM, UEBA, Data Classification, SWG, and ZTNA** to help organisations:

Discover, classify, and protect personal data across endpoints, SaaS, and cloud.

Prevent unauthorised copying, sharing, or exfiltration of personal data.

Enforce least-privilege and secure access policies.

Maintain audit-ready logs for regulators.

Automate workflows for deletion, retention, and access requests.

How Kitecyber Product(s) and Feature(s) Successfully Map into GDPR Checklist

GDPR Requirement	Mapped Kitecyber Product(s) & Feature(s)	How Kitecyber Helps
Lawful, fair, and transparent processing	DLP, Compliance Workflows	DLP tracks processing activities; compliance workflows link data to consent; generates subject-level reports.
Purpose limitation	DLP, Data Classification	AI-driven classifiers tag data by purpose; DLP ensures processing aligns with declared purpose.
Data minimisation	DLP, UEM	DLP prevents unnecessary duplication; UEM enforces endpoint policies to limit data collection.
Accuracy	DLP, Compliance Dashboards	DLP tracks records and changes; dashboards alert on outdated or inconsistent data.
Storage limitation	UEM, DLP, Compliance	Remote wipe, retention policies, and automated device reset workflows ensure data is removed when no longer needed.
Integrity and confidentiality	DLP, SWG, UEBA, ZTNA	DLP prevents exfiltration; SWG blocks malicious web/SaaS access; UEBA detects anomalous behavior; ZTNA enforces secure access.
Accountability & governance	DLP, UEM, Audit Logs	Maintains logs of all data processing events; UEM enforces device compliance; audit-ready reports simplify GDPR audits.
Data subject rights	DLP, Compliance Workflows	Automated workflows handle access, correction, erasure, and portability requests; DLP provides visibility across systems.
Breach notification	DLP, UEBA, Audit Logs	Detects unauthorized access or leaks; UEBA prioritizes incidents; audit logs provide evidence for reporting within 72 hours.
Privacy by design & by default	DLP, Data Classification, ZTNA, UEM	Classifies personal data before processing; ZTNA enforces least-privilege access; UEM ensures secure device posture; DLP prevents unauthorized use by default.

Practical Benefits of Kitecyber for GDPR Compliance

Comprehensive coverage

Protects personal data across endpoints, cloud apps, SaaS, and networks.

Automated data subject rights workflows

Reduces manual effort and compliance risk.

Audit-ready reporting

Simplifies GDPR audits and regulator reporting.

Preventative controls

DLP, SWG, and ZTNA prevent breaches before they occur.

Continuous monitoring

UEBA and DLP detect anomalous behavior and insider threats in real time.

Quick Checklist to Start with Kitecyber

1. **Discover and classify personal data** across endpoints, cloud, and SaaS.
2. **Deploy DLP policies** for access, sharing, and deletion.
3. **Enable UEM controls** for device encryption, patching, and access posture.
4. **Implement ZTNA** for least-privilege access to sensitive applications.
5. **Monitor user activity** with UEBA for anomalous behavior.
6. **Generate audit-ready logs** for GDPR compliance verification.

KITE CYBER

Kitecyber, 691 S Milpitas Blvd, Ste 217, Milpitas, CA 95035
Email: info@kitecyber.com
Website: www.kitecyber.com

LinkedIn Twitter YouTube