



B2B SAAS PLATFORM

# LudiSec

---

WHITEPAPER

GDPR Compliance Checklist for SMEs

## Document Information

---

|                       |               |
|-----------------------|---------------|
| <b>Published</b>      | June 10, 2026 |
| <b>Uploaded</b>       | 2026-06-10    |
| <b>Author</b>         | Joan Fontbona |
| <b>Classification</b> | Public        |

# Executive Summary

---

## WHAT THIS GUIDE COVERS

This expanded checklist is designed for Small and Medium-sized Enterprises (SMEs) operating within the EU or processing EU citizen data. It covers the core pillars of GDPR readiness, moving beyond basic compliance to robust operational resilience.

## CHECKLIST

### Data Inventory and Mapping:

- Conduct a comprehensive data mapping exercise identifying all personal data collected, stored, and processed.
- Document the specific lawful basis for each processing activity (e.g., explicit consent, legitimate interest, contract fulfillment).
- Define and enforce strict data retention schedules, ensuring automated deletion of records past their legal necessity.

### Consent and User Rights Management:

- Implement granular, unbundled consent mechanisms on all digital platforms, strictly avoiding pre-ticked boxes.
- Document a clear, tested Subject Access Request (SAR) procedure capable of delivering user data within the 30-day legal window.
- Verify the Right to Erasure workflow across both active production databases and offline archival backups.

### Breach Response and Incident Handling:

- Establish a 72-hour notification procedure to your national supervisory authority for critical data exposure.
- Maintain a detailed internal breach register for all incidents, even those not meeting the external reporting threshold.
- Train IT and frontline staff on rapid breach identification, escalation, and containment protocols.

### Risk Assessments and DPO Requirements:

- Conduct Data Protection Impact Assessments (DPIAs) before deploying any new high-risk processing technologies or large-scale tracking.
- Determine if your core activities require appointing a dedicated Data Protection Officer (DPO) based on systematic monitoring criteria.

### Staff Training and Accountability:

- Complete mandatory annual GDPR awareness training for all employees regardless of department.
- Deliver specialized, role-specific privacy training for data processors handling sensitive health or financial information.
- Maintain signed, timestamped training records as a primary defense measure for external compliance audits.

## CONCLUSION

GDPR compliance is a continuous operational requirement, not a one-time audit project. For SMEs, regular

staff training and strict data minimalism remain the most cost-effective defensive controls against devastating regulatory fines.

## 1. Introduction

*This whitepaper outlines the essential GDPR compliance steps tailored specifically for Small and Medium-sized Enterprises (SMEs).*

## 2. Background & Context

*Since its implementation in 2018, GDPR has reshaped data privacy. SMEs often struggle with the complexity of these regulations compared to larger enterprises with dedicated legal teams.*

## 3. Methodology

*We aggregated data from 500 SME compliance audits to identify the most common gaps and practical remediation strategies.*

## 4. Findings

*72% of SMEs lack proper data mapping, and 55% have inadequate breach reporting mechanisms.*

## 5. Recommendations

*Implement a continuous data inventory process, enforce strict consent management, and conduct annual staff training.*

## 6. Conclusion



*GDPR compliance is an ongoing operational requirement, not a one-time audit checklist. Continuous training is your best defense.*

## 7. References

---

1. Official Journal of the European Union, Regulation (EU) 2016/679. 2. EDPB Guidelines on Consent.



## About LudiSec

LudiSec is a cybersecurity risk management platform headquartered in Barcelona, Spain. Serving enterprise clients across financial services, healthcare, manufacturing, and the public sector. Available in English, Spanish, and Catalan.