



PLATAFORMA SAAS B2B

LudiSec

WHITEPAPER

Llista de Verificació de Compliment GDPR per a PYMEs



Informació del document

Publicat	June 10, 2026
Pujat	2026-06-10
Autor	Joan Fontbona
Classificació	Publica

Resum Executiu

QUÈ COBREIX AQUESTA GUIA

Aquesta llista de verificació ampliada està dissenyada per a Petites i Mitjanes Empreses (PIMES) que operen dins la UE o processen dades de ciutadans de la UE. Cobreix els pilars centrals de la preparació per al GDPR, anant més enllà del compliment bàsic cap a una resiliència operativa sòlida.

LLISTA DE VERIFICACIÓ

Inventari i Mapatge de Dades:

- Realitzar un exercici integral de mapatge de dades identificant totes les dades personals recopilades, emmagatzemades i processades.
- Documentar la base legal específica per a cada activitat de processament (per exemple, consentiment explícit, interès legítim, compliment de contracte).
- Definir i fer complir estrictes cronogrames de retenció de dades, assegurant l'eliminació automatitzada de registres passada la seva necessitat legal.

Consentiment i Gestió de Drets d'Usuari:

- Implementar mecanismes de consentiment granulars i desglossats en totes les plataformes digitals, evitant estrictament les caselles premarcades.
- Documentar un procediment de Sol·licitud d'Accés de l'Interessat (SAR) clar i provat, capaç de lliurar les dades de l'usuari dins del termini legal de 30 dies.
- Verificar el flux de treball del Dret a l'Oblit tant en bases de dades de producció actives com en còpies de seguretat d'arxiu fora de línia.

Resposta a Bretxes i Gestió d'Incidents:

- Establir un procediment de notificació de 72 hores a l'autoritat de control nacional per a l'exposició crítica de dades.
- Mantenir un registre intern detallat de bretxes per a tots els incidents, fins i tot aquells que no assoleixen el llindar de notificació externa.
- Capacitar el personal de TI i de primera línia en protocols ràpids d'identificació, escalada i contenció de bretxes.

Avaluacions de Risc i Requisits del DPO:

- Realitzar Avaluacions d'Impacte de Protecció de Dades (AIPD) abans d'implementar qualsevol nova tecnologia de processament d'alt risc o seguiment a gran escala.
- Determinar si les seves activitats principals requereixen el nomenament d'un Delegat de Protecció de Dades (DPO) dedicat segons els criteris de monitoratge sistemàtic.

Capacitació del Personal i Responsabilitat:

- Completar la capacitació obligatòria anual de conscienciació sobre el GDPR per a tots els empleats, independentment del departament.
- Impartir formació especialitzada en privadesa específica del rol per als processadors de dades que manegen informació financera o de salut sensible.
- Mantenir registres de capacitació signats i amb marca de temps com a mesura de defensa principal per a auditories de compliment externes.



CONCLUSIÓ

El compliment del GDPR és un requisit operatiu continu, no un projecte d'auditoria únic. Per a les PIMEs, la capacitat regular del personal i l'estricta minimalisme de dades continuen sent els controls defensius més rendibles contra les devastadores multes regulatòries.

1. Introducció

Aquest document tècnic descriu els passos essencials de compliment del GDPR adaptats específicament per a petites i mitjanes empreses (PIMEs).

2. Marc i context

Des de la seva implementació el 2018, el GDPR ha remodelat la privadesa de dades. Les PIMEs sovint lluiten amb la complexitat d'aquestes regulacions en comparació amb les grans empreses.

3. Metodologia

Vam agregar dades de 500 auditories de compliment de PIMEs per identificar les bretxes més comunes i estratègies pràctiques de remediació.

4. Troballes

El 72% de les PIMEs no tenen un mapatge de dades adequat, i el 55% tenen mecanismes inadequats de notificació de bretxes.

5. Recomanacions

Implementar un procés continu d'inventari de dades, fer complir una gestió estricta del consentiment i realitzar formació anual del personal.

6. Conclusions

El compliment del GDPR és un requisit operatiu continu, no una llista de verificació d'auditoria única. La formació contínua és la vostra millor defensa.

7. Referències

1. Diari Oficial de la Unió Europea, Reglament (UE) 2016/679. 2. Directrius del CEPD sobre el consentiment.



Sobre LudiSec

LudiSec és una plataforma de gestió de riscos de ciberseguretat amb seu a Barcelona, Espanya. Serveix a clients empresarials de serveis financers, sanitat, indústria manufacturera i el sector públic. Disponible en anglès, castellà i català.