Digital Marketing Spain

GDPR & LOPDGDD Website Compliance Guide for Estate Agents in Spain

A PRACTICAL GUIDE FOR BRITISH & INTERNATIONAL AGENCIES

Written by:
Anthony S Rose

Presented by:
Digital Marketing Spain

Legal Disclaimer

This guide is provided exclusively for general informational and educational purposes. It does not constitute legal advice and should not be used as a substitute for consulting with a qualified GDPR/LOPDGDD specialist or legal professional.

No Advisory Relationship

Downloading, reading, or using this guide does not create any advisory, professional, or client relationship between you and the author or Digital Marketing Spain.

Not Tailored to Your Circumstances

Data protection law is highly fact-specific. Every estate agency has unique circumstances, tools, processes, and risk profiles that affect compliance requirements. This guide provides general guidance but cannot address your specific situation.

No Guarantee of Compliance

Following the recommendations in this guide does not guarantee compliance with GDPR, LOPDGDD, or other applicable laws. Compliance depends on correct implementation of principles to your specific context, which may require professional assessment.

Law Changes

Data protection law and regulatory guidance evolve continuously. While this guide reflects current understanding as of publication, subsequent developments may affect the accuracy or completeness of information provided.

No Liability

No liability whatsoever is accepted for any actions taken or not taken based on the contents of this guide. You are solely responsible for ensuring your own compliance with applicable laws and regulations.

Recommendation

For advice relating to your specific circumstances, systems, and processes, you must consult an appropriately qualified and accredited professional specialising in GDPR and Spanish data protection law.

Regulatory Authority

For official guidance, consult the Spanish Data Protection Agency (AEPD) at www.aepd.es or seek qualified legal counsel.

Table of Contents

Table of Contents II

How to Use This Guide

Who This Is For

This guide is designed for estate agents operating in Spain, particularly British and international agencies serving expat communities. If you have a website that collects personal data (and you almost certainly do), this guide will help you understand your basic obligations.

What It Covers

*T*he primary focus is on website compliance - the area where most estate agents face immediate risk and where clarity is most needed. However, GDPR and LOPDGDD extend far beyond websites, so we'll also highlight broader obligations you should be aware of.
How to Read This

You can approach this guide in two ways:

1. **Quick Scan:** Read the headings and highlighted sections to get an overview of key requirements.
2. **Deep Dive:** Work through each section carefully, using the Checklist section to audit your own website.

What Happens Next

This guide gives you the knowledge to identify potential gaps. It doesn't make you compliant, only proper implementation and, where necessary, professional guidance can do that. Think of this as your foundation for informed decision-making.

A Note on Language

We've kept technical jargon to a minimum, but some terms are unavoidable. Check the Glossary section if you encounter unfamiliar terminology.

Why GDPR Matters for Your Estate Agency

The Reality of Data Collection

As an estate agent, you collect personal data constantly:

- Names, phone numbers, and email addresses from website forms
- Property preferences and financial capability from valuation requests
- Identity documents for formal offers and AML compliance
- Location data and browsing behaviour through analytics
- Messages and conversations through WhatsApp and chat widgets

This isn't incidental to your business, and it's central to it. Every lead, every enquiry, every viewing request involves personal data.

The Digital Exposure

Your website is often your first point of contact with potential clients. It's also where compliance failures are most visible and most easily discovered. Common issues include:

- Contact forms collecting data without proper privacy information
- Cookie banners that don't actually block tracking
- WhatsApp buttons with no explanation of how data will be used
- Analytics running before users give consent
- Requests for excessive information (like DNI numbers for simple enquiries)

Real Enforcement

The Spanish Data Protection Agency (AEPD) doesn't just issue theoretical guidelines, they actively investigate and sanction estate agents. Real cases include:

- Fines for publishing photos showing personal items in inhabited properties
- Sanctions for collecting DNI copies unnecessarily
- Penalties for cookie banners that don't offer genuine choice
- Enforcement action for privacy policies that don't match reality

Fines for small-to-medium estate agencies can reach several thousand euros and, in more serious cases, tens of thousands of euros. The exact amount depends on the seriousness of the breach, previous history, and the level of cooperation with the AEPD.

The Business Case for Compliance

*B*eyond avoiding fines, compliance offers tangible benefits:

- **Trust:** Clients handling major life transactions value agencies that take privacy seriously
- **Professionalism:** Proper data handling reflects operational maturity
- **Risk reduction:** Clear processes prevent accidental breaches

Competitive advantage: In a trust-driven market, visible compliance matters

The Bottom Line

You don't need to become a data protection expert, but you do need to understand the basics. This guide will show you what those basics are.

The Legal Framework You Need to Know

GDPR: The European Foundation

Core GDPR Principles:

1. **Lawfulness, Fairness, Transparency**: You must have a legal reason to process data and be open about what you're doing
2. **Purpose Limitation**: Data collected for one purpose can't be freely used for another
3. **Data Minimisation**: Only collect what you actually need
4. **Accuracy**: Keep information correct and up to date
5. **Storage Limitation**: Don't keep data longer than necessary
6. **Integrity and Confidentiality**: Protect data from unauthorised access or loss
7. **Accountability**: You must be able to demonstrate compliance

LOPDGDD: The Spanish Layer

Spain's Organic Law 3/2018 (LOPDGDD) supplements the GDPR with Spain-specific requirements. Key additions relevant to estate agents include:

- More detailed rules on video surveillance (CCTV in offices)
- Specific provisions for processing data of deceased persons
- Additional protections for minors
- The Spanish sanctioning regime and enforcement procedures

Who Enforces This?

In Spain, the AEPD (Agencia Española de Protección de Datos) is the authority responsible for enforcement. They investigate complaints, conduct audits, and impose sanctions.

Your Role: The "Controller"

In GDPR terminology, your estate agency is a "data controller." This means:

- You decide what data to collect and why
- You choose which tools and systems to use (website platform, CRM, analytics)
- You determine how long to keep data
- You're ultimately responsible for compliance, even when using third-party services

The Critical Concept: Proactive Responsibility

The GDPR requires "accountability" i.e the ability to demonstrate compliance, not just claim it. This means:

- Having written policies that reflect what you actually do
- Keeping records of your data processing activities
- Documenting consent and legal bases
- Maintaining contracts with service providers
- Being able to show this documentation if the AEPD asks
- It's no longer enough to say "we're compliant." You must be able to prove it.

Legal Bases for Processing

You need a lawful reason to process personal data. The main ones relevant to estate agents are:

1. **Consent**: The person has explicitly agreed (e.g., ticking a box for marketing emails)
2. **Contract**: Processing is necessary to provide the service requested (e.g., arranging a viewing)
3. **Legal Obligation**: Required by law (e.g., AML identity checks for transactions)
4. **Legitimate Interest**: Necessary for your business interests, provided these don't override the person's rights (use with caution and document carefully)
5. Different activities require different legal bases. Your privacy policy should specify which basis applies to each type of processing.

Your Website Privacy Notice

What It Must Include

The AEPD requires the following information:

1. Identity and Contact Details

- Your legal entity name (not just your trading name)
- Registered address
- Contact email or phone number
- If you've appointed a Data Protection Officer (DPO), their contact details

2. Purposes of Processing Be specific about why you collect data:

- ✓ "To respond to your property enquiry"
- ✓ "To arrange a viewing at the property you selected"
- ✓ "To send you property alerts matching your preferences (with consent)"
- ✗ "For commercial purposes" (too vague)

3. Legal Basis For each purpose, state your lawful basis:

- "Consent of the interested party"
- "Performance of a contract"
- "Legal obligation (Anti-Money Laundering Law 10/2010)"
- "Legitimate interest in maintaining business records"

4. Recipients of Data Who else sees the data? List categories or specific entities:

- "Your enquiry may be shared with the property owner or their representative"
- "We use [CRM Name] to manage client relationships"
- "Property listings are published on Idealista and Fotocasa"
- "Email communications are sent via [Provider Name]"

If you don't share data with anyone, state: "We do not share your data with third parties except where legally required."

5. International Transfers If you use services based outside the European Economic Area (like some US-based email platforms or cloud storage), you must explain:

- Where the data goes
- What safeguards are in place (e.g., "EU-US Data Privacy Framework," "Standard Contractual Clauses")

6. Retention Periods How long you keep data:

- "Transaction data: 10 years (Anti-Money Laundering obligations under Law 10/2010)"
- "Enquiry data where no transaction occurs: many agencies opt for a retention period of around 1–2 years of inactivity, but you should define and document a period that is appropriate for your agency and can be justified"
- "Marketing consent: until you unsubscribe"
- Be realistic. Don't claim you delete data after 30 days if you actually keep it for years in your CRM.

7. Data Subject Rights Explain that users can:

- Access their data
- Correct inaccurate information
- Request deletion (with limitations for legal obligations)
- Object to processing
- Withdraw consent at any time
- Lodge a complaint with the AEPD
- Provide a clear method to exercise these rights (email address or contact form).

8. Automated Decision-Making If you use automated systems to make decisions about people (unlikely for most estate agents), you must disclose this.

Best Practice: The Layered Approach

Modern compliance uses two layers:

First Layer (Short Summary):

- Appears directly on forms, at point of data collection
- Provides essential information at a glance
- Includes link to full policy
-

Second Layer (Complete Policy):

- Comprehensive document on dedicated page
- Contains all required legal detail
- Accessible from every page (footer link)

Example First Layer Text (for a contact form):

Data Protection Information

Controller: Costa Sol Properties S.L. | Purpose: To respond to your enquiry | Legal Basis: Your consent | Recipients: Data is not shared with third parties except service providers | Rights: Access, rectify, delete your data by contacting info@example.com | More info: [Privacy Policy]

This approach prevents "privacy fatigue" while ensuring transparency.

Common Mistakes to Avoid

- Using a generic template that doesn't reflect your actual practices
- Listing services you don't use or omitting ones you do
- Vague language about purposes or retention
- No mention of your CRM, analytics, or marketing tools
- Privacy policy that hasn't been updated in years

Your privacy policy must be a living document that accurately describes your real data practices.

Note: If your business is Spanish (S.L. or Autónomo), your legal texts (Aviso Legal/Privacy Policy) must be available in Spanish to be legally valid for the AEPD, even if your clients are British. Having an English translation is great for service, but the Spanish version is the legal shield.

Cookie Compliance & Consent

What Are Cookies?

The AEPD requires the following information:

Cookies are small files stored in a visitor's browser. They serve various purposes: remembering login details, analysing site traffic, delivering personalised ads, and tracking user behaviour across websites.

Why They Matter for GDPR

Most cookies involve processing personal data (IP addresses, browsing behaviour, device identifiers). Under GDPR and Spanish law, this processing requires compliance with strict rules.

The 2023/2024 AEPD Guidance

The Spanish Data Protection Agency has updated its cookie guidance to align with EU-wide standards. The rules are now very clear and heavily enforced.
Cookie Categories

1. Strictly Necessary (Technical) Cookies

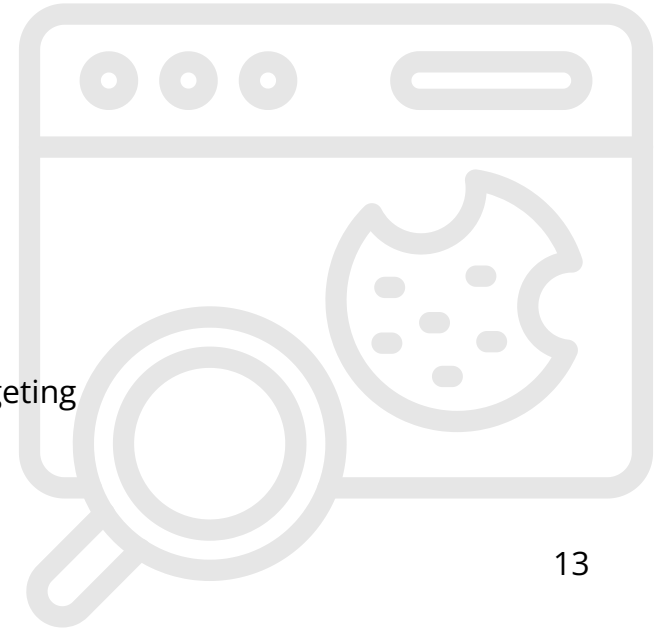
- Essential for the website to function
- Examples: security tokens, load balancing, session management
- No consent required
- Can be set automatically

2. Analytical/Performance Cookies

- Measure website usage and performance
- Examples: Google Analytics, GA4, Matomo
- Consent required before activation
- Must allow users to opt out

3. Marketing / Advertising Cookies

- Track users for targeted advertising
- Examples: Facebook Pixel, Google Ads retargeting
- Consent required before activation
- Must be clearly identified



4. Personalisation Cookies

- Remember user preferences
- Language selection (without consent if user selects it)
- Consent depends on what's being personalised

Your Cookie Banner Must:

1. Appear Before Cookies Load The banner must display on the first visit, and non-essential cookies must not activate until consent is given. Simply showing a banner while cookies run in the background is non-compliant.

2. Offer Equal Choice The "Accept All" and "Reject All" buttons must be:

- The same size
- The same visual prominence
- The same colour intensity
- Equally easy to click

Common Violation: A big green "Accept All" button with "Reject All" hidden in a "Settings" menu or shown in gray text as a small link.

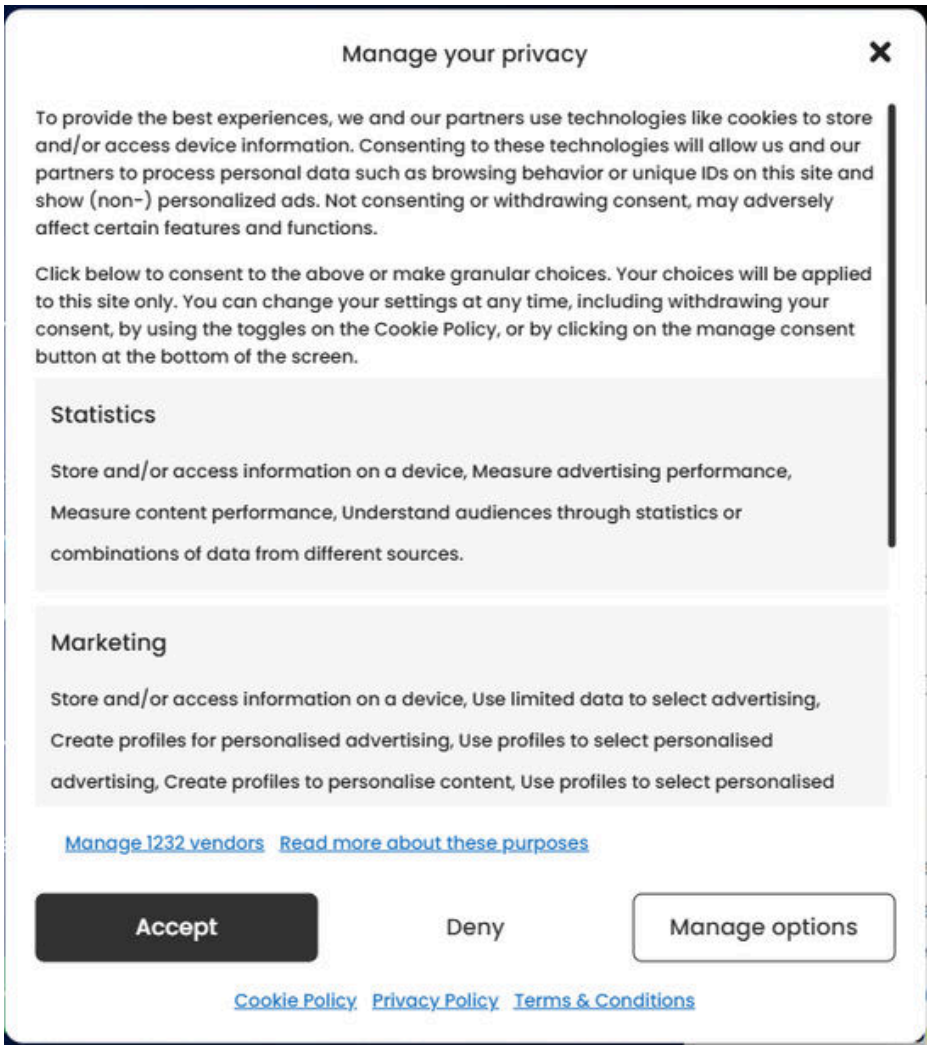
3. Allow Granular Control Users must be able to:

- Accept all
- Reject all
- Choose specific categories (e.g., accept analytics but reject marketing)

4. Not Use "Dark Patterns" Prohibited practices include:

- Making "Reject" harder to find or requiring extra clicks
- Using confusing languag
- Forcing users to accept cookies to access content (unless cookies are genuinely necessary for the service)
- Automatically accepting cookies after a time delay

5. Remember Choice Once a user makes a selection, don't ask again on every page visit. However, the AEPD's guidance suggests you should prompt again after a reasonable period (often in the region of 6–12 months) or if you make significant changes to your cookies or tracking tools.



Example of a properly configured consent banner

What "Reject All" Really Means

When a user clicks "Reject All":

- Only strictly necessary cookies can be set
- No analytics should run
- No marketing pixels should fire
- No behavioural tracking should occur

Many cookie banners fail here, they show the right buttons but don't actually enforce the user's choice. This is a serious compliance failure.

Your Cookie Policy Page

In addition to the banner, you need a separate page explaining:

- What cookies your site uses
- What each cookie does
- How long each cookie lasts
- Which are necessary vs. optional
- How users can manage or delete cookies via browser settings

Common Tools and How to Configure Them

Google Analytics / GA4:

- Must not load before consent
- Should use Consent Mode V2 (Google's framework for respecting user choice)
- Consider GA4 with IP anonymization and data retention limits

Facebook Pixel:

- Requires explicit consent before loading
- Must be in "marketing" or "advertising" category
- Users who reject must not be tracked

Example of Compliant Flow:

1. User lands on website
2. Cookie banner appears immediately
3. No analytics or marketing scripts have loaded yet
4. User clicks "Reject All"
5. Only technical cookies are set
6. Google Analytics never initializes for this visitor
7. User can browse normally

Non-Compliant Flow:

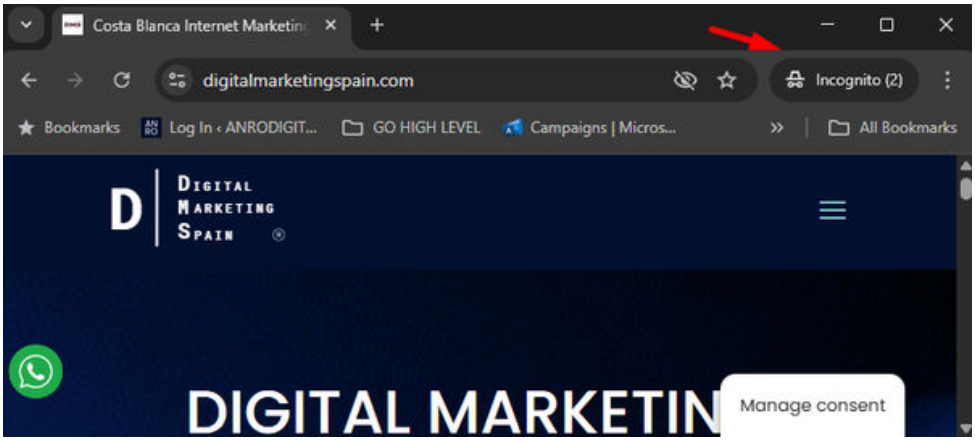
1. User lands on website
2. Google Analytics is already running
3. Cookie banner appears (but damage is done)
4. User clicks "Reject All"
5. Tracking stops, but initial data was already collected without consent

The Sanction Risk

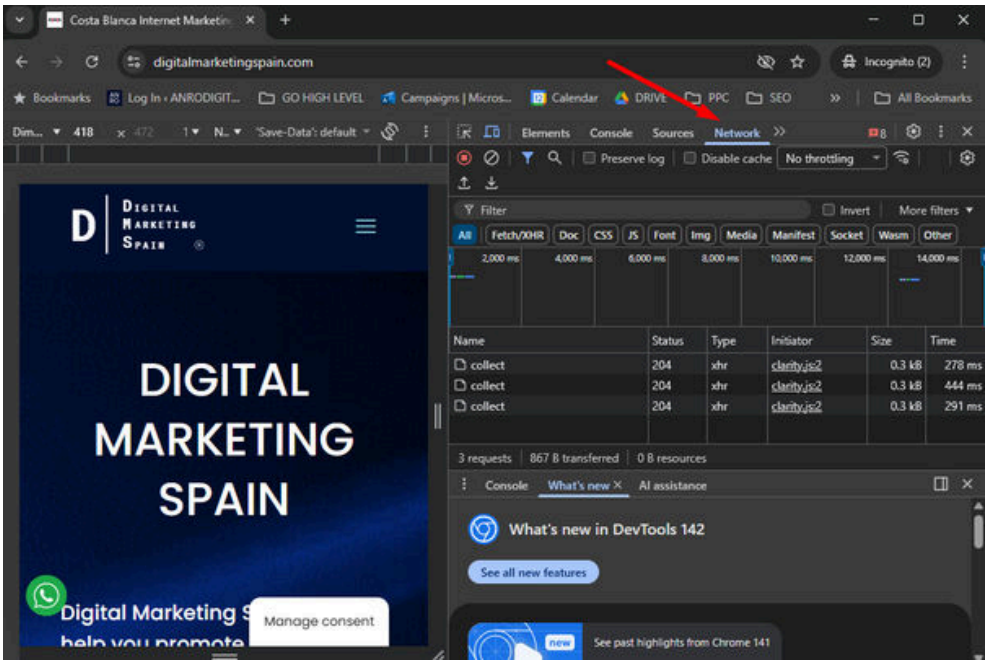
Cookie compliance failures are among the most common reasons for AEPD investigations. Sanctions in past cases have ranged from several thousand to tens of thousands of euros for agencies. The violations are easy to detect, the AEPD or complainants simply need to visit your website and inspect browser behavior.

How to Check if Your Cookie Banner is Compliant

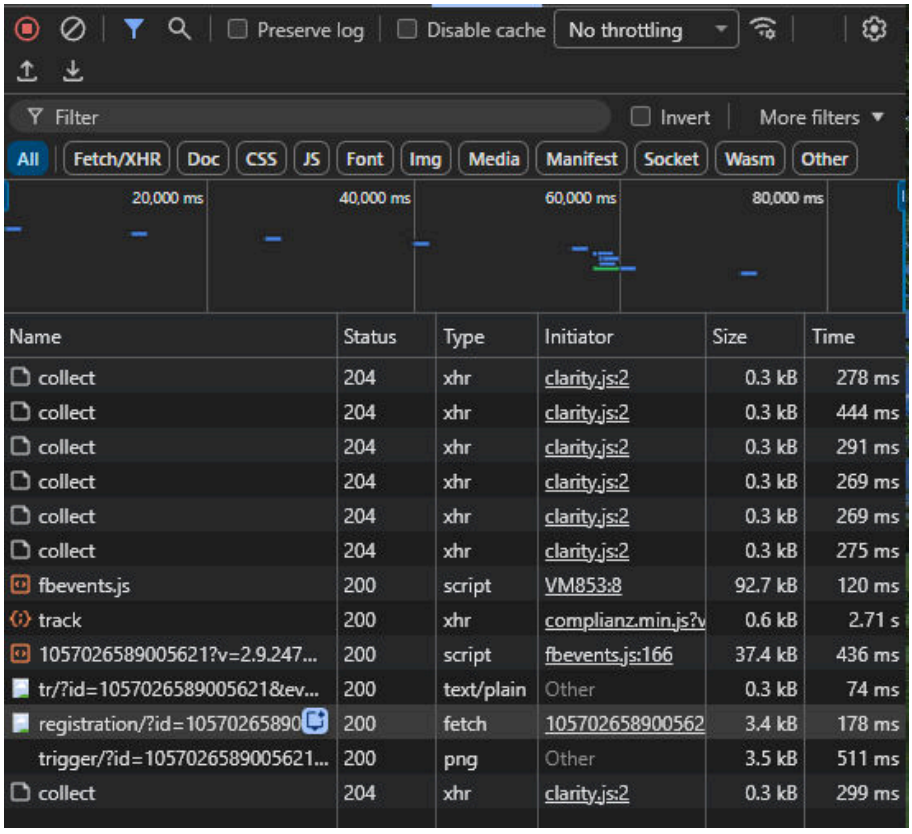
1. Visit your website in incognito browser mode



Open browser developer tools in Google Chrome (F12 → Network or Application tab)



If you see nothing as in the above then nothing is being tracked,
in the case of DigitalMarketingSpain.com, tracking was blocked by the cookies plugin.



If you see as in the above images words like track or fbevents, before you accept the cookies then you have a problem

Website Forms & Data Collection

The Entry Point for Most Data

Contact forms, property enquiry forms, valuation requests, and newsletter sign-ups are where most visitors become data subjects. Getting these right is critical.
What Must Be Visible on Every Form

Before a user clicks "Submit," they must see:

1. Privacy Information Either the full First Layer summary or, at minimum:
- Link to your privacy policy
- Statement of purpose: "We'll use this information to [respond to your enquiry / send you property alerts / arrange a viewing]"
- Legal basis for processing

2. Clear Purpose Statement Users need to know exactly what they're signing up for:
- ✓ "We'll contact you about the property at Ref: 12345"
- ✓ "We'll send you an estimated market value for your property"
- ✗ "To process your request" (too vague)

3. Consent Mechanism Where Required If you want to use the data for marketing beyond the immediate request, you need a separate, optional checkbox:
- ✗ "By submitting, you agree to our privacy policy and to receive marketing" (conflates acceptance of policy with marketing consent)
- ✓ "□ I'd like to receive property alerts and news" (optional, unchecked by default, separate from the core service)

The DNI Problem

Why It's Problematic:

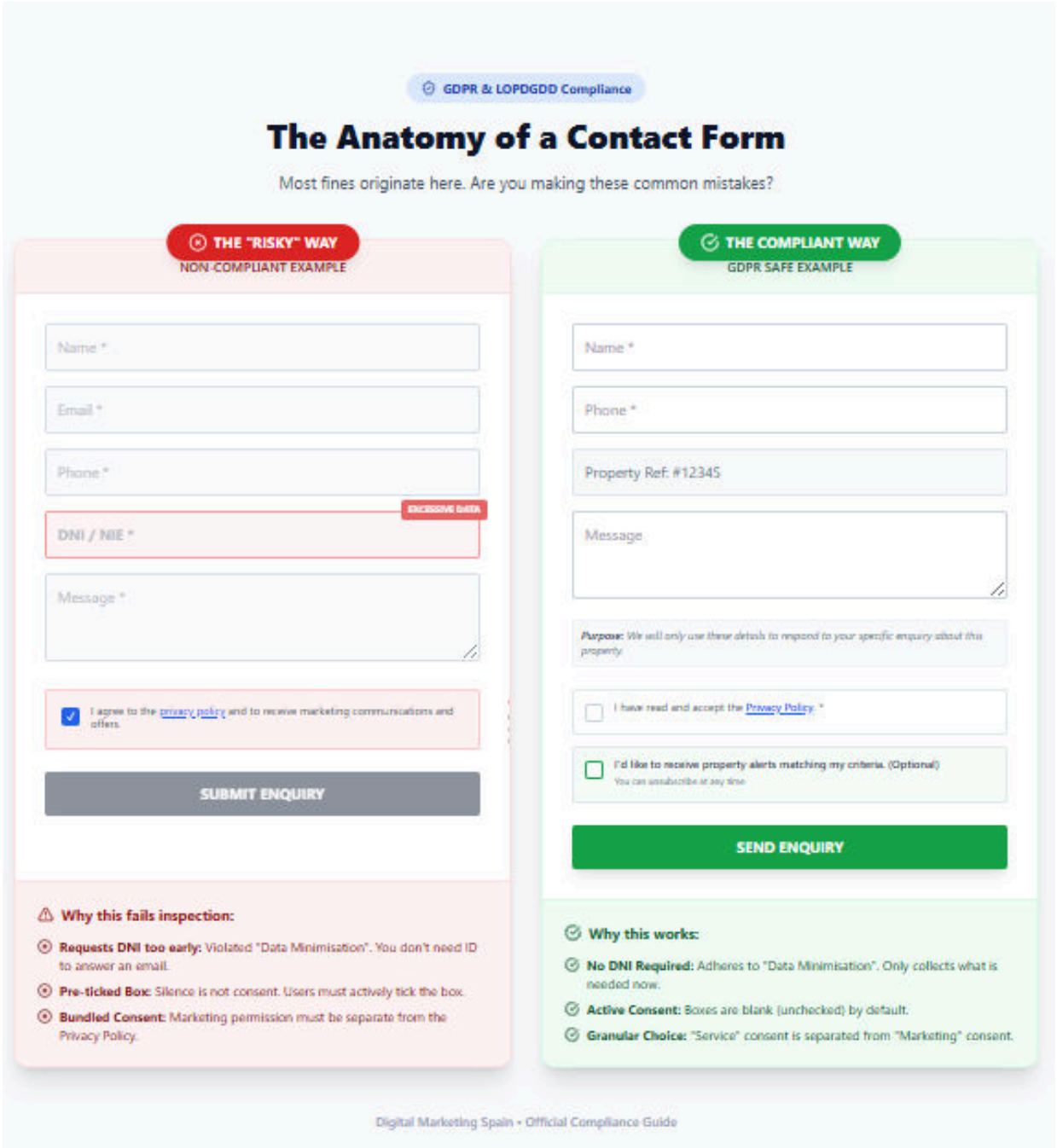
- Asking for a DNI to book a viewing or request property information violates the principle of data minimisation
- The AEPD has specifically sanctioned agencies for this practice
- You don't need someone's DNI to show them a house

When You CAN Request DNI:

- When submitting a formal purchase offer
- When legally required for Anti-Money Laundering (AML) checks (i.e., when a transaction is likely to proceed)
- When signing a reservation contract

What to Ask Instead: For initial enquiries and viewings, name, phone, and email are sufficient. You can always collect additional information later in the process when it's genuinely needed.

Sanction Risk: Past cases of excessive data collection at inappropriate stages have resulted in fines ranging from several thousand to tens of thousands of euros.



Form Security

Examples of appropriate security measures include:

- Using HTTPS (secure connection, you should see the padlock in the browser)
- Not transmitting data over unencrypted connections
- Protection against spam/bots (CAPTCHA or similar)
- Avoiding sending sensitive data via unencrypted email

Hidden Fields and Tracking
Many forms include hidden fields that capture:

- IP address
- Referral source (where the visitor came from)
- Device type
- Time of enquiry

This is generally acceptable but should be mentioned in your privacy policy under "Information Collected Automatically."

The Newsletter Checkbox

If you offer property alerts or newsletters:

- Must be a separate, unchecked checkbox
- Must clearly explain what they'll receive ("weekly email with new properties matching your criteria")
- Must be optional (form submission shouldn't be blocked if they don't check it)
- Must include easy unsubscribe method in every email sent

WhatsApp, Chat Widgets & CRM Integration

WhatsApp Buttons

BWhatsApp has become essential for estate agents serving international clients. However, clicking a WhatsApp link immediately shares the user's phone number with your business WhatsApp account and potentially WhatsApp/Meta's servers.

What You Must Do:

Before the User Clicks: Display information warning them what will happen:

- "By contacting us via WhatsApp, you agree to share your phone number with us and the processing of your data according to our privacy policy [link]"

This notice should appear:

- Next to the WhatsApp button
- Or in a hover tooltip
- Or as an interstitial (pop-up) when they click, requiring confirmation

In Your Privacy Policy: Explicitly mention WhatsApp as a communication channel and explain that conversations may be stored in your business account for service records.

Security Consideration:

- It is strongly advisable to avoid sending identity documents or financial information via WhatsApp
- If you must, use WhatsApp Business with end-to-end encryption and document this in your security procedures
- Avoid using personal WhatsApp accounts for business communications, you have no control over data retention or security on personal devices

Chat Widgets (Live Chat & AI Chatbots)

Many estate agency websites now feature chat functionality, with either live human support or AI-powered bots.

Compliance Requirements:

1. Disclosure Before Chat Starts Users should see:

- Whether they're chatting with a human or a bot
- That their messages and contact details will be processed
- Link to privacy policy

2. Data Flow Transparency Most chat widgets send data to third-party providers (e.g., Drift, Intercom, Tidio, or custom AI solutions). Your privacy policy must:

- Name the chat provider
- Explain where data is stored
- Note if conversations are recorded or analysed

3. AI-Specific Considerations If using AI chatbots:

- Disclose that AI is being used
- Explain if conversations train the AI model
- Consider whether the AI provider uses data for their own purposes (many do, so read their terms carefully)

4. Data Processing Agreements You need a signed agreement with your chat provider confirming they're a "processor" acting on your instructions.

CRM Systems: The Central Compliance Challenge

Your CRM (Customer Relationship Management system) is where most client data ultimately resides. Common platforms for Spanish estate agents include Inmovilla, Witei, Go High Level, and various international systems.

Key Compliance Points:

1. You Are the Controller Even though the CRM provider hosts the data, you control what goes into it and how it's used. This means:

- You're responsible if data is misused
- You decide retention periods
- You must respond to data subject requests

2. Data Processing Agreement (DPA) Required Under Article 28 of the GDPR, you must have a written contract with your CRM provider that specifies:

- What data they process on your behalf
- That they only process according to your instructions
- Security measures they've implemented
- What happens to data if you stop using the service
- Their obligation to assist with data breaches or regulatory requests

Most reputable CRM providers offer standard DPAs. If yours doesn't, that's a red flag.

3. Transparency in Privacy Policy Your privacy policy must mention that you use a CRM to manage client relationships. You don't necessarily need to name the specific product, but stating "We use customer relationship management software to track enquiries and maintain records" is essential.

4. Data Location Know where your CRM data is stored:

- EU/EEA: Generally no additional concerns
- UK: Now considered adequate by the EU
- US: Requires safeguards (EU-US Data Privacy Framework or Standard Contractual Clauses)
- Other countries: May require specific approvals or safeguards
-

If data is stored outside the EU, this must be disclosed in your privacy policy with details of safeguards.

5. Access Controls Examples of good practice include:

- Limiting access based on job role
- Using strong passwords
- Enabling two-factor authentication if available
- Logging access for audit purposes

Portal Integrations (Idealista, Fotocasa, Kyero)

When you list properties on portals, data flows in both directions.

Outbound (Your Listings to Portals):

- You control the property data you send
- Be careful about publishing property owner information
- Remove personal items from photos before uploading

I**nbound (Leads from Portals to You):**

- The portal typically collects the enquiry under their own privacy policy
- They then pass it to you as a "referral"
- Your privacy policy should note "We receive enquiries from property portals including [list major ones]"
- When you receive a lead, process it according to your own privacy policy from that point forward

Understanding the Relationship:

- Portals usually act as independent controllers for users browsing properties
- You become the controller when the lead is passed to you
- Document where leads come from in your CRM (useful for demonstrating lawful processing if questioned)

API Integrations and Automation

Many agencies use automation to sync data between:

- Website forms → CRM
- CRM → Email marketing platform
- Portal leads → CRM

Each integration should be:

- Documented (you should know exactly what data flows where)
- Covered by appropriate agreements with service providers
- Mentioned in your privacy policy if it affects user data

Photography & Inhabited Properties

A Specific Spanish Risk Area

The AEPD has been particularly active in sanctioning estate agents for privacy violations related to property photography. This section deals with a uniquely sensitive aspect of real estate: marketing someone's home while respecting their privacy.

Why This Matters

A photograph of an empty room is not personal data. But a photograph of a lived-in space that reveals information about the occupant, their lifestyle, family composition, economic status, health, religion, or political views, is processing personal data under GDPR.

What the AEPD Has Sanctioned

Real cases include:

- Family photographs visible on shelves or walls
- Children's drawings or photos on refrigerators
- Visible medications or medical equipment
- Religious items (crucifixes, prayer mats, religious texts)
- Personal mail or documents in view
- Distinctive personal belongings that could identify occupants

The Legal Problem:

- Data Minimisation Violation: These personal details are not necessary to market the property
- Special Category Data: Images of minors receive heightened protection
- Lack of Consent: Occupants (especially tenants) may not have consented to their personal life being broadcast online

Typical Sanction Range: In past cases involving property photography violations, particularly those involving minors, sanctions have reached tens of thousands of euros.

What You Must Do Before Photography

1. Pre-Photography Protocol It is strongly advisable to develop a checklist for agents and photographers:

- Request occupants remove all personal photos and items
- Check bathrooms for medications or personal products
- Verify children's rooms have no identifying items
- Ask about religious or cultural items that should be removed
- Consider scheduling when occupants can be present

2. Post-Photography Review Before publishing:

- Review every photo carefully
- Blur or crop out any missed personal items
- Use editing tools to remove visible documents or identifiable objects
- When in doubt, err on the side of caution

3. Virtual Staging Alternative For sensitive properties or uncooperative occupants, consider:

- AI-powered virtual staging (digitally furnishing empty spaces)
- Wide-angle shots that minimise personal detail
- External photos only until viewing stage
-

Tenant Rights vs. Owner Rights

This creates a legal tension:

The Owner has a legitimate right to market and sell their property.

The Tenant has a constitutional right to privacy and the "inviolability of the domicile."
The Balance:

- Owners can list the property for sale
- Tenants cannot unreasonably prevent viewings or photos
- But tenants can refuse to have their personal belongings photographed for public listing
- Viewings must be arranged at reasonable times with proper notice

Practical Solutions:

- Negotiate a photography session where tenant's personal items are temporarily stored
- Use virtual staging for furnished visualization
- Focus on property features (kitchen, bathroom, structural elements) rather than occupied living spaces
- Limit photos to empty rooms or owner-occupied spaces only

The Viewing Process

When conducting viewings of tenant-occupied properties:

- Provide reasonable advance notice to tenants (Spanish rental law typically requires 24-48 hours)
- Respect the tenant's privacy during visits
- Don't photograph inside during viewings unless specifically agreed
- Don't share tenant information with potential buyers unless necessary and consented

Geolocation and Exact Addresses

Publishing the precise address of a property can constitute processing personal data if it allows identification of the owner through public records.

Risks:

- High-value properties: security risk (theft, targeting)
- Vulnerable individuals
- Public figures seeking discretion

Best Practice:

- Use general location for initial listings: "Marbella Old Town," "Nueva Andalucía Golf Valley"
- Provide specific address only to serious, vetted applicants
- Consider this especially for luxury properties

This isn't a strict legal requirement, but it demonstrates good data protection practice and duty of care to clients.

Common Risk Areas & How to Fix Them

This section identifies the most frequent compliance failures among Spanish estate agents and provides practical solutions.

ES RGPD/LOPD Compliance Risk Audit

Identification of vulnerabilities and strategic solutions for Digital Marketing Spain.

Group 1: HIGH and MEDIUM-HIGH Priority Risks

These risks require immediate attention and represent the highest potential for substantial regulatory fines.

COMPLIANCE ISSUE	RISK	CONSEQUENCES AND PRECEDENTS	IMMEDIATE STRATEGIC SOLUTION
Cookie banner DOES NOT block analytics or tracking scripts.	HIGH	Sanctions ranging from several thousand to tens of thousands of euros. Consent is invalid if tracking occurs beforehand.	**Action:** Implement a Consent Management Platform (CMP) that genuinely prevents scripts from loading until consent is given. Always test in incognito mode.
Requesting National ID (DNI) on initial inquiry/viewing forms.	HIGH	Fines in past cases have reached tens of thousands of euros. DNI is a special category of data at the initial stage.	**Action:** Remove DNI from all initial contact/inquiry forms. Only collect when legally required (formal offers, AML checks).
Personal items visible in property photos.	HIGH (Minors)	Serious cases have resulted in substantial fines, especially if there are images of minors or sensitive data.	**Action:** Establish a photo review protocol. Remove or blur personal items. Never publish images showing children or sensitive data.
Office CCTV cameras filming the public street.	HIGH	Has resulted in substantial fines in past cases due to excessive capture.	**Action:** Adjust camera angles to only capture the interior. Display compliant signage and register with AEPD if required.
Absence of visible privacy information on forms.	MEDIUM-HIGH	Frequent sanctions in the thousands of euros range for non-compliance with the duty to inform.	**Action:** Add a First Layer Summary (Short Clause) to every form. Include purpose, controller identity, and a link to the full policy.

Group 2: MEDIUM and LOW Priority Risks

These risks should be addressed in the short to medium term to ensure full legal adherence and avoid future sanctions.

COMPLIANCE ISSUE	RISK	CONSEQUENCES AND PRECEDENTS	IMMEDIATE STRATEGIC SOLUTION
Pre-ticked marketing consent boxes.	MEDIUM	Enforcement cases with fines ranging from several thousand to tens of thousands of euros. Consent must be freely given and explicit.	**Action:** Ensure all marketing consent checkboxes are unchecked by default. They must be a genuinely opt-in option.
Generic, vague, or outdated Privacy Policy.	MEDIUM	AEPD actions resulting in significant fines if policies do not reflect the actual practices of the company.	**Action:** Update the policy to reflect reality. Include specific retention periods, name the CRM/tools, and reflect all processing activities.
Lack of Data Processing Agreements (DPA) with vendors.	MEDIUM	Can result in sanctions in the thousands or tens of thousands of euros range. It is a legal obligation when hiring services that access data.	**Action:** Obtain signed DPAs from all service providers (CRM, email marketing, hosting, etc.) who access client data.
Use of personal WhatsApp for business communications.	MEDIUM	Security risk, lack of traceability, and potential sanction. Personal and professional data are mixed.	**Action:** Migrate to WhatsApp Business. Never send ID documents. Establish a data/conversation retention policy.
No HTTPS (secure connection) on the website.	MEDIUM	Considered an inadequate technical security measure for handling data.	**Action:** Install an SSL/TLS certificate. Ensure all pages (especially forms) load under https://.
Marketing emails without an 'Unsubscribe' option.	MEDIUM	Past cases have resulted in fines in the thousands or tens of thousands of euros for non-compliance with LSSI and RGPD.	**Action:** Include a clear and unmistakable 'Unsubscribe' link in every marketing email. Process unsubscribe requests immediately.
Indefinite data retention ('just in case').	LOW-MEDIUM	Can result in sanctions, particularly when combined with other violations.	**Action:** Implement a documented retention schedule. Delete or anonymize data according to defined and legally justified periods.

The Pattern

Most sanctions share common features:

- The violation was easily visible (public website, published photos)
- The agency couldn't demonstrate compliance when asked
- There was no documented policy or procedure
- The response to AEPD enquiries was slow or inadequate

Prevention Strategy

The majority of these risks can be mitigated with:

1. Initial audit of your website and practices
2. Documentation of what you do and why
3. Training staff on data protection basics
4. Regular review (annually at minimum)
5. Quick response to any AEPD communications

When Things Go Wrong

If you receive an AEPD communication:

- **Do not ignore it** (this dramatically increases sanctions)
- **Respond within stated deadlines** (usually 10 business days for initial response)
- **Cooperate fully** (provide requested documentation)
- **Fix the issue immediately** (demonstrates good faith)
- **Consider professional representation** (data protection lawyers can negotiate and reduce penalties)

The difference between a smaller fine and a substantially larger one is often cooperation and remediation during the investigation process.

Beyond Websites - What Else GDPR Covers

Important Context

This guide has focused on website compliance because that's where most estate agents face immediate, visible risk. However, it's crucial to understand that GDPR and LOPDGDD apply to all processing of personal data, not just what happens online.

The Full Scope of Estate Agency Data Processing

Your obligations extend to:

1. Paper Records & Physical Documents

- Viewing sheets (Hoja de Visita)
- Signed contracts and reservation agreements
- Copies of identity documents
- Financial documentation
- Property valuation reports
- Client files in filing cabinets

Requirements:

- Secure storage (locked cabinets, restricted access)
- Retention schedules (know when to shred)
- Privacy information on any forms signed by clients

2. Anti-Money Laundering (AML) Compliance Estate agents are "obligated subjects" under Spanish AML law (Law 10/2010).

Obligations:

- Verify client identity for transactions
- Conduct due diligence on beneficial owners
- Report suspicious transactions
- Keep records for 10 years (this is a legal requirement, not optional)

GDPR Interaction:

- Processing for AML is based on legal obligation, not consent
- You must do it even if clients object
- But you can only use this data for AML purposes, not marketing
- Must be mentioned in your privacy policy

3. Office CCTV (Video Surveillance) Spanish law (LOPDGDD Article 22) has specific rules:

Requirements:

- Display information signs (cartel de videovigilancia) at all entrances
- Signs must identify the controller and where to exercise rights
- Cameras must focus only on your own property - never public streets
- Footage typically kept for 1 month maximum
- May need to register with AEPD depending on circumstances

Common Mistake: Positioning cameras to monitor the street outside for security. This is prohibited, only state security forces can film public spaces.

4. Email Marketing & Newsletters If you send property alerts or promotional emails:
Requirements:

- Based on explicit consent (opt-in)
- Clear unsubscribe option in every email
- Unsubscribe requests processed within 24-48 hours
- Don't pre-tick sign-up boxes
- Keep records of when and how consent was obtained

5. Staff Data & HR Your employees' personal data is also protected:

What You Process:

- Employment contracts
- Payroll information
- Performance reviews
- Bank details
- Identity documents

Requirements:

- Confidentiality agreements signed by all staff
- Secure storage of personnel files
- Clear HR privacy policy
- Limited access to sensitive information

6. Data Sharing with Third Parties Beyond your CRM and website tools, you may share data with:

Notaries: For deed preparation (legal necessity, must inform clients)
Banks/Mortgage Brokers: For financing (usually requires specific consent unless the bank is a pure processor)

Appraisers (Tasadoras): For property valuations (legitimate interest or contractual necessity)

External Accountants (Gestorías): For tax and administrative services (processor relationship, need DPA)

Other Agents: For co-listing or referrals (requires transparency and often consent)
Property Owners: Sharing buyer information (usually contractual necessity, but be careful about excessive detail)

7. Portals and Lead Sources When leads come from Idealista, Fotocasa, or other portals:

Understand:

- The portal collected data under their policy
- They're passing it to you
- You become the controller from that point
- You must handle according to your own privacy policy
- Good practice: send a welcome email confirming your privacy approach

8. International Transfers If you use services with servers outside the EU:
Common Examples:

- US-based email marketing (Mailchimp, Constant Contact)
- US cloud storage (Dropbox, Google Drive in some configurations)
- US CRM systems
- Some video conferencing tools

Requirements:

- Verify the legal basis for transfer (adequacy decision, standard contractual clauses, or other safeguards)
- Disclose in privacy policy
- Ensure service provider has appropriate protections

9. Data Breaches A breach isn't just a cyberattack. It includes:
Physical:

- Lost laptop or mobile phone with client data
- Documents left in a taxi
- Files stolen during break-in
- Set of keys labelled with property address

Digital:

- Ransomware or hacking
- Email sent to wrong recipient
- Accidental publication of personal data
- Cloud account compromise

Obligations:

- Document all breaches in an internal register
- Assess risk to individuals
- If there's a risk: notify AEPD within 72 hours
- If there's a high risk: notify affected individuals without delay
- Take immediate steps to mitigate harm

10. Security Measures You must implement appropriate technical and organizational security. Examples of appropriate measures include:

Technical:

- Strong passwords (consider using a password manager)
- Two-factor authentication where available
- Encrypted devices (especially laptops and mobiles)
- Regular backups
- Updated software and security patches
- Antivirus and firewall protection

Organisational:

- Clear desk policy (don't leave documents visible)
- Screen privacy (lock computers when leaving desk)
- Access controls (not everyone needs access to everything)
- Staff training on phishing and social engineering
- Incident response plan

The Breadth of Compliance

This section demonstrates that GDPR compliance is a comprehensive operational framework, not just a website checkbox. While your website is the most public and easily scrutinised aspect, the AEPD can investigate any aspect of your data handling.

Strong Recommendation

Given the complexity and breadth of these obligations, most estate agencies benefit from professional guidance. A qualified GDPR/LOPDGDD specialist can:

- Conduct a full audit of your practices
- Draft compliant documentation
- Implement appropriate security measures
- Provide ongoing compliance monitoring
- Represent you in case of AEPD investigation

This guide gives you the foundation to understand what's required. Professional advice helps you implement it correctly for your specific circumstances.

Your Website Compliance Checklist

Use this checklist to audit your own website. Each item represents a key requirement discussed in this guide.

Privacy Information

□ Privacy policy accessible from every page (typically in footer)
□ Controller identity clearly stated (legal entity name, not just brand)
□ All purposes of data processing listed specifically (not vague terms)
□ Retention periods specified and justified
- 10 years for AML/transaction data (legal requirement)
- Document your chosen periods for other data types

□ User rights clearly explained (access, rectification, deletion, objection, complaint)
□ Third-party processors identified
- CRM system named or described
- Analytics mentioned (Google Analytics, etc.)
- Email marketing platform if used
- Other services that access data

□ International transfers disclosed (if using non-EU services, with safeguards explained)
□ Contact method for data protection enquiries provided

Cookies & Tracking

□ Cookie banner appears on first visit (before any non-essential cookies load)
□ "Accept All" and "Reject All" buttons equally visible and prominent
□ No analytics or marketing cookies load before consent (test this in incognito mode)
□ Granular control available (users can accept some categories, reject others)
□ Cookie policy page exists and is comprehensive
- Lists all cookies used
- Explains purpose of each
- States duration
- Identifies which are necessary vs. optional

□ Settings allow users to change their preferences later
□ No "cookie walls" (users can reject and still access content)

Website Forms (Contact, Valuation, Newsletter)

□ Privacy information visible at each form (First Layer summary or clear link)
□ Link to full privacy policy present and functional
□ DNI is NOT requested for enquiries or viewing requests
□ Purpose clearly stated for each form
- "To respond to your property enquiry"
- "To provide an estimated valuation"
- Not vague terms like "commercial purposes"

□ Marketing consent is separate and optional
- Separate checkbox from form submission
- Unchecked by default
- Clear explanation of what they'll receive

□ No pre-ticked boxes (all optional consents must be user-initiated)
□ HTTPS enabled across entire site (check URL shows https:// and padlock icon)
□ Forms protected against spam (CAPTCHA or similar)

Third-Party Tools & Integrations

□ CRM system mentioned in privacy policy
□ Data processing agreement (DPA) signed with CRM provider
□ WhatsApp button includes privacy notice
- Users warned before clicking
- Explains data sharing
- Links to privacy policy

□ Chat widget (if present) properly disclosed
- Users know if it's AI or human
- Privacy information provided before chatting
- Provider identified in privacy policy

□ Google Analytics configured correctly
- Only loads after consent
- Consider using Consent Mode V2
- IP anonymization enabled if possible

□ Facebook Pixel or other tracking pixels require consent before loading
□ Portal integrations documented
- Privacy policy notes you receive leads from portals
- Process for handling inbound leads is clear

Property Listings & Photography

□ Photos checked for personal items before publication
□ No images of minors or family photos visible
□ Personal medications, documents, or identifying items removed or blurred
□ Religious or culturally sensitive items considered
□ Tenant privacy respected in occupied property listings
□ Exact addresses used cautiously (consider using general area for initial listings)

General Good Practices

□ Staff trained on basic data protection principles
□ Clear process for handling data subject requests (access, deletion, etc.)
□ Documented retention schedule exists
□ Data breach response protocol in place
□ Regular review schedule established (at least annually)
□ Devices secured (passwords, encryption, locked screens)
□ Access to data restricted (not everyone in office needs access to everything)
□ Physical documents stored securely (locked cabinets for client files)
□ Confidentiality agreements signed by all staff

How to Use This Checklist

1. Go through each item systematically
2. Check items you're confident about
3. Mark items you're unsure about for investigation
4. Note items that clearly aren't in place
5. Prioritize fixes based on risk (DNI collection, cookie compliance, missing privacy info are high priority)
6. Document your review (date completed, who reviewed, findings)
7. Create action plan for gaps identified
8. Schedule next review (6-12 months)

Important Note

This checklist is a tool for self-assessment and education. A fully checked list doesn't guarantee absolute compliance, that requires professional evaluation of your specific circumstances.

However, addressing these items will significantly improve your compliance posture and reduce risk.

Key Terms Explained

AEPD (Agencia Española de Protección de Datos)
Spain's Data Protection Agency. The authority responsible for enforcing GDPR and LOPDGDD in Spain, investigating complaints, and imposing sanctions.

AML (Anti-Money Laundering)
Regulations requiring estate agents to verify client identity and maintain records for transactions. This is a legal obligation under Spanish Law 10/2010, creating a mandatory 10-year data retention requirement.

Consent
Freely given, specific, informed, and unambiguous agreement to data processing. Must be opt-in (not pre-ticked), easy to withdraw, and documented. One of several possible legal bases for processing.

Controller
The entity (your estate agency) that determines the purposes and means of processing personal data. You decide what data to collect, why, and how. You're responsible for compliance.

Cookie
A small file stored in a user's browser. Can be "necessary" (technical, no consent required) or "non-essential" (analytics, marketing, requiring consent).

Data Breach
Any incident where personal data is accidentally or unlawfully accessed, lost, destroyed, altered, or disclosed. Includes both digital (hacking) and physical (lost documents) incidents.

Data Processing Agreement (DPA)
A contract required between a controller (you) and processor (service provider) under Article 28 GDPR. Specifies what data the processor handles, security obligations, and data protection responsibilities.

Data Subject
The individual whose personal data is being processed. In estate agency context: potential buyers, sellers, tenants, property owners, website visitors.

Data Subject Rights
Rights that individuals have under GDPR including: right to access their data, right to rectification (correction), right to erasure ("right to be forgotten"), right to object to processing, right to data portability, right to restrict processing.

GDPR (General Data Protection Regulation)
EU Regulation 2016/679, effective from May 2018. The primary data protection law applying across the European Union, including Spain.

International Transfer
Sending personal data outside the European Economic Area (EEA). Requires appropriate safeguards such as adequacy decisions, Standard Contractual Clauses, or other approved mechanisms.

Lawful Basis (Legal Basis)
The legal justification for processing personal data. Must be one of six options in Article 6 GDPR. Most relevant for estate agents: consent, contract, legal obligation, legitimate interest.

Legitimate Interest
One possible legal basis for processing. Allows processing necessary for legitimate business purposes, provided these don't override individual rights. Requires careful balancing test and documentation. Often misunderstood—not a free pass for any processing.

LOPDGDD (Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales)
Spain's Organic Law 3/2018 on Data Protection and Guarantee of Digital Rights. Supplements GDPR with Spain-specific requirements and clarifications.

Personal Data
Any information relating to an identified or identifiable individual. Includes obvious identifiers (name, email, phone, address) and less obvious ones (IP address, device ID, cookie identifiers, location data).

Processor
A service provider that processes personal data on behalf of a controller according to the controller's instructions. Examples: CRM provider, cloud storage company, email marketing platform, external accountant.

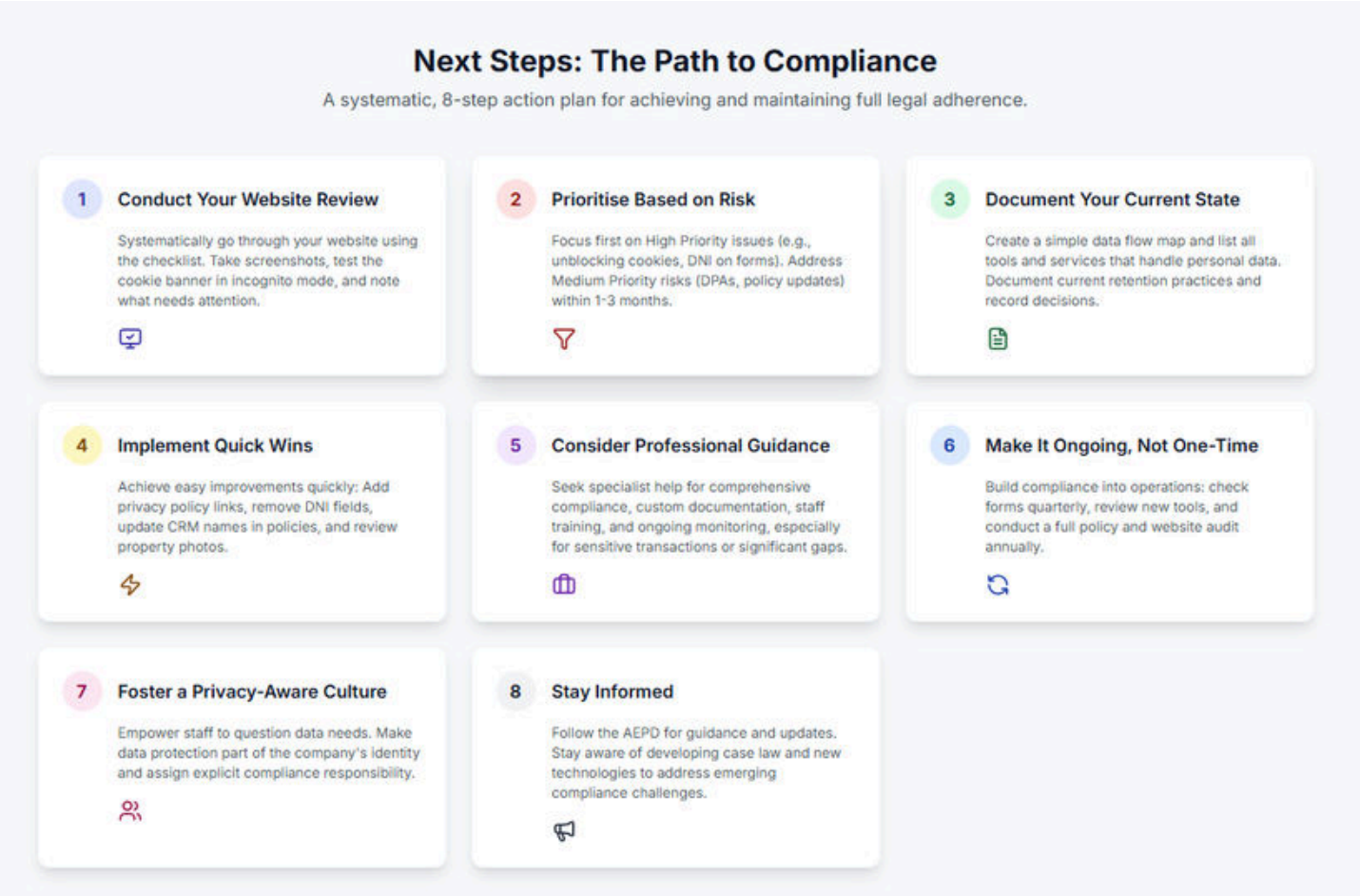
Proactive Responsibility (Accountability)
GDPR principle requiring organizations to not only comply but be able to demonstrate compliance through documentation, policies, and records. You must prove you're compliant, not just claim it.

Retention Period
How long data is kept. Must be specified in privacy policy and based on legitimate need. Should be defined and documented based on legal requirements and business justification.

Special Category Data (Sensitive Data)
Data revealing racial or ethnic origin, political opinions, religious beliefs, health, sex life, or biometric data. Requires heightened protection and usually explicit consent. Estate agents rarely need to process this deliberately but may capture it accidentally in property photos.

Third Country
Any country outside the European Economic Area (EEA). Transfers of data to third countries require additional safeguards.

Transparency
Core GDPR principle requiring clear, accessible, understandable information about data processing. Users must know what you're doing with their data, in language they can understand.



Most importantly, view data protection not as a burden, but as a responsibility to the people who trust you with their personal information during one of the most significant transactions of their lives.

Your clients are sharing their dreams, their financial situations, their family circumstances. Treating that information with respect and care isn't just a legal obligation, it's a professional and ethical one.

You've taken the first step by educating yourself. Now take the next step by putting that knowledge into action.

Final Disclaimer

Important Legal Notice

This guide is provided exclusively for general informational and educational purposes. It does not constitute legal advice and should not be used as a substitute for consulting with a qualified GDPR/LOPDGDD specialist or legal professional.

No Advisory Relationship
Downloading, reading, or using this guide does not create any advisory, professional, or client relationship between you and the author or Digital Marketing Spain.

Not Tailored to Your Circumstances
Data protection law is highly fact-specific. Every estate agency has unique circumstances, tools, processes, and risk profiles that affect compliance requirements. This guide provides general guidance but cannot address your specific situation.

No Guarantee of Compliance
Following the recommendations in this guide does not guarantee compliance with GDPR, LOPDGDD, or other applicable laws. Compliance depends on correct implementation of principles to your specific context, which may require professional assessment.

Law Changes
Data protection law and regulatory guidance evolve continuously. While this guide reflects current understanding as of publication, subsequent developments may affect the accuracy or completeness of information provided.

No Liability
No liability whatsoever is accepted for any actions taken or not taken based on the contents of this guide. You are solely responsible for ensuring your own compliance with applicable laws and regulations.

Recommendation
For advice relating to your specific circumstances, systems, and processes, you must consult an appropriately qualified and accredited professional specializing in GDPR and Spanish data protection law.

Regulatory Authority
For official guidance, consult the Spanish Data Protection Agency (AEPD) at www.aepd.es or seek qualified legal counsel.

About This Guide

This GDPR & LOPDGDD Website Compliance Guide was created by Anthony Rose as an educational resource for the estate agent community in Spain.
Anthony Rose works in digital marketing and has a particular focus on privacy safe marketing. This guide is provided solely for educational purposes and does not form part of any professional service.

The goal is to demystify complex regulations and provide practical, accessible information that helps estate agents understand their obligations and take meaningful steps toward compliance.

Digital Marketing Spain

info@digitalmarketingspain.com

Version Information

Version 1.0 | December 2025