FOR UK ESTATE AND LETTING AGENTS UNDER HMRC AML SUPERVISION

The AML and KYC *Compliance Checklist*

A plain English run through of what HMRC's Money Laundering Regulations 2017 require an estate or letting agent business to have in place, the records that prove it, and the bits agents most often get pulled up on at a supervisory visit.

01 · WHO THIS APPLIES TO

Both sides of the property transaction, both rental thresholds.

HMRC supervises estate agency businesses (acting for buyers and sellers in property sales) and letting agency businesses (where a single contract is for a rent of **10,000 euro per month or more**). Both branches need separate registration. The high value dealer rules also apply if you take cash payments of 10,000 euro or more in a single or linked transaction.

- **Sales agents** are in scope from the moment they take instructions, on both vendor and prospective purchaser sides.
- **Letting agents** are in scope only above the 10,000 euro per month threshold, but firm wide controls still apply across the whole agency.
- **Auctioneers and online platforms** facilitating property transfers are in scope on the same basis as estate agents.

02 · FIRM WIDE RISK ASSESSMENT

The document HMRC asks for first.

A written assessment of how money laundering and terrorist financing risks present in your firm, given your customer base, the products and services you offer, the geographies you operate in, your delivery channels, and the transactions you typically handle. Reviewed at least annually and after any material change.

> **The record HMRC pulls agents up on most.**
>
> Visits regularly find good per customer due diligence files but no documented firm wide risk assessment behind them. Without it the rest of the regime has nothing to size itself against, and HMRC treats that as a structural failure rather than a paperwork miss.

03 · POLICIES, CONTROLS AND PROCEDURES (PCPS)

Five written documents, proportionate to the firm.

1. **AML policy** stating how the firm meets the Regulations, signed off by senior management.
2. **Customer due diligence procedure** covering identification, verification, beneficial ownership, source of funds, ongoing monitoring.
3. **Suspicious activity reporting procedure** naming the nominated officer (MLRO) and the internal reporting path.
4. **Training procedure** covering induction, refresher cadence, the topics covered, and how attendance is recorded.
5. **Record keeping procedure** covering what is kept, where, for how long, and who has access.

04 · CUSTOMER DUE DILIGENCE PER INSTRUCTION

Identify, verify, understand, record.

Identify the customer (vendor or purchaser, lessor or tenant) by full legal name, date of birth, residential address.

Verify from a reliable independent source. One government photo ID plus one recent (3 month) proof of address as a minimum, more for higher risk.

Understand beneficial ownership where the customer is a company, trust or partnership. Anyone with 25% plus control needs identifying and verifying in their own right.

Source of funds for the transaction must be plausibly explained and where elevated risk, evidenced.

Ongoing monitoring through the life of the instruction, including for changes in circumstance, behaviour or transaction pattern.

Politically exposed persons (PEPs) require enhanced due diligence and senior management sign off before the relationship begins.

Sanctions screening against the OFSI consolidated list at the start of every instruction and on each new beneficial owner identified.

Refuse or terminate if CDD cannot be completed. Document the decision either way.

05 · ENHANCED DUE DILIGENCE TRIGGERS

Higher scrutiny is mandatory in these cases.

- A politically exposed person, family member, or known close associate.
- A customer based in, or with funds from, a high risk third country on the HMT list.
- A complex or unusually large transaction with no apparent economic or legal purpose.
- A non face to face customer where remote ID verification is the only check.
- Any other circumstance the firm wide risk assessment flags as higher risk.

06 · RECORD KEEPING

Five years from the end of the business relationship.

All CDD documents, transaction records, internal SAR considerations, training logs, and the firm wide risk assessment reviews are kept for at least five years after the relationship ends, or after the transaction completes for one off instructions. Records must be retrievable on request.

07 · NOMINATED OFFICER (MLRO) AND SARS

One person owns suspicious activity reporting.

A nominated officer (often the MLRO) receives internal disclosures, decides whether to file with the National Crime Agency, and is the firm's external SAR signatory. Internal disclosures, the decision, and any external SAR reference are all kept on file. Staff training must make the internal reporting path obvious.

08 · TRAINING AND OVERSIGHT

Induction, refresh, log it.

All relevant staff trained on the firm's AML obligations at induction and refreshed at least annually. The training covers the firm's PCPs, red flags relevant to the business, the internal reporting path, and the sanctions framework. Attendance and content kept on the training log.

The two minute self check.

Can you produce, today, on request: (1) the firm wide risk assessment in writing, (2) the five PCP documents signed off by senior management, (3) the CDD file for the last instruction, with ID, address proof, beneficial ownership and source of funds, (4) the SAR consideration log, (5) the training log for the last two years, (6) the five year record retrieval test? If any of those would be a scramble, the AML and KYC Document Pack covers the documents already done.