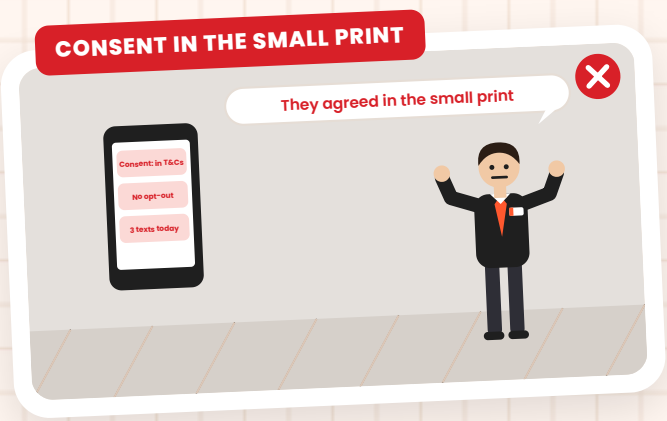
autosmart

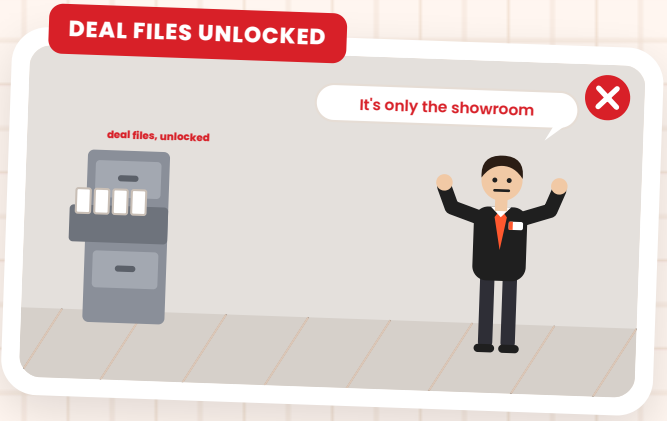
Edition 1 · United Kingdom · 2026

• £17.5M OR 4% OF TURNOVER Marketing, website, deal files, CRM & service data

Data Protection Compliance Guidebook for Automotive Companies

Marketing consent, cookies, privacy notices, access requests, security and retention: what the ICO checks, **and why marketing fines just went up 35 times.**





£17.5M
or 4% of turnover: now the ceiling for **marketing and cookie** breaches too (Feb 2026).

170M
car finance claim texts behind the ICO's **search warrants** (Jul 2026).

72 hours
to report a serious data breach to the ICO.

7 standards · 20 checkpoints · UK GDPR · DPA 2018 · PECR · Right way / wrong way · Ideal fix time

2022 Car finance firm · £60K → **Feb 2026** PECR fines × 35 → **Jul 2026** ICO search warrants → **Marketing fines now match GDPR fines.**

WHY THIS GUIDEBOOK EXISTS

Dealers hold more personal data than most banks see.

Driving licences, payslips, bank details, addresses, vehicle and telematics data: a dealership collects it all and shares it with lenders, manufacturers and insurers. Since **5 February 2026**, the Data (Use and Access) Act has raised marketing and cookie fines to the GDPR ceiling of **£17.5M or 4% of turnover**.

This guidebook covers the 7 data standards that matter most in a dealership.

WHERE THE DATA RISK SITS

Marketing
Emails, texts and calls
DAT-01

Website
Cookies and tracking
DAT-02

Transparency
Privacy notices and sharing
DAT-03

Customer rights
Access and deletion requests
DAT-04

Security
Deal files and systems
DAT-05

Housekeeping
Retention and ICO fee
DAT-06 · 07

WHO ENFORCES IT

ICO
Information Commissioner's Office
Fines, enforcement notices, search warrants

Courts
County and High Court
Customer compensation claims

FCA
Joint taskforce
Car finance claims marketing (with ICO, ASA, SRA)

Manufacturers
OEM data agreements
Contract terms on shared customer data

WHO IT'S FOR

Dealer principals & directors
Understand the new marketing fine ceiling.

Marketing, sales & service
Know what consent and notices must look like.

DPOs & auditors
Test consent, cookies and requests like the ICO would.

MARKETING FINES JUST WENT UP 35×

From £500,000 to £17.5 million. For a text message.

Until February 2026, the most the ICO could fine for unlawful marketing was **£500,000**. The Data (Use and Access) Act raised it to **£17.5M or 4% of global turnover**, the same as the worst GDPR breaches.

THE PENALTY LADDER

LEVEL 1
£4,350
Fixed penalty: ICO fee not paid.

LEVEL 2
Notice
Enforcement notice: stop marketing or processing.

LEVEL 3
£8.7M / 2%
Security and record-keeping failures.

LEVEL 4
£17.5M / 4%
Consent, transparency, marketing and cookies.

REAL CASES FROM US AUTOMOTIVE BUSINESSES

WHO	RESULT	WHAT HAPPENED
Car finance claims marketers ICO · Jul 2026	**170M texts** 12M+ complaints	Search warrants in Bolton, Burnley, Liverpool, London and Swansea.
Finance Giant ICO · Apr 2022	**£60,000** under the old cap	Car sales finance firm: consent forced through terms, no opt-out.
Nuisance marketing firms ICO · Jan 2026	**£225,000** combined fines	Unsolicited marketing messages.

OLD MARKETING CAP
£500K
Before 5 Feb 2026.

NEW MARKETING CAP
£17.5M
Or 4% of global turnover, whichever is higher.

AND THEN
Claims
Customers can **sue for compensation**.

HOW TO USE THIS GUIDE

One page per standard. Consent is everything.

1. **Header**: code, area, owner and the maximum penalty
2. **The law**: which regulator and which regulation
3. **The cost**: fine, what else can happen and a real case
4. **Right / wrong**: illustrated pass and fail, plus how to audit

THE 7 STANDARDS

DAT-01	Marketing Consent	PECR reg.22	CRITICAL	£17.5M / 4%	Immediate	5
DAT-02	Cookie Consent	PECR reg.6	CRITICAL	£17.5M / 4%	7 days	6
DAT-03	Privacy Notice & Lawful Basis	UK GDPR a.13	CRITICAL	£17.5M / 4%	30 days	7
DAT-04	Subject Access Requests	UK GDPR a.15	CRITICAL	£17.5M / 4%	7 days	8
DAT-05	Security & Breach Reporting	UK GDPR a.32–33	CRITICAL	£8.7M / 2%	24 hours	9
DAT-06	Retention & Disposal	UK GDPR a.5(1)(e)	CRITICAL	£17.5M / 4%	30 days	10
DAT-07	ICO Fee Paid	DPA 2018 Regs	MODERATE	£4,350	7 days	11

IDEAL FIX TIME · COUNTED FROM AUDIT SUBMISSION

Immediate	Stop now · serious harm or clear breach	1 standard
24 hours	Fix within 1 working day	1 standard
7 days	Fix within 1 week · records, notices, training	3 standards
30 days	Plan and close within 1 month · policies and systems	2 standards

SCORING EACH CHECKPOINT

PASS
Every criterion met at the time of audit, with evidence captured.

FAIL
Any criterion not met at the time of audit. Record what you saw and who owns the fix.

N/A
Only where "Applies when" rules it out. Record why.

Note. Data shared with manufacturers under OEM agreements still needs a lawful basis and must appear in your privacy notice.

DAT-01 DATA PROTECTION · ICO · STANDARD 01 OF 07

Marketing Consent

Area **Marketing · CRM** | Person in charge **Marketing Manager · DPO** | Regulator **ICO**

MAXIMUM PENALTY

GBP 17.5M

or 4% of global turnover, if higher

Since 5 Feb 2026 the same ceiling applies to **marketing & cookies**

• CRITICAL

THE LAW

UK GDPR

UK GDPR · **Data Protection Act 2018** · **PECR 2003** as amended by the **Data (Use and Access) Act 2025** · **PECR regs 21–22** electronic marketing · soft opt-in rules

WHAT WE CHECK

Marketing emails and texts go only to customers who opted in, or existing customers under the soft opt-in with an easy opt-out every time. Consent is never forced through terms and conditions.

CHECKPOINTS IN THE AUDIT

- Q1 Is marketing consent collected separately, not bundled into terms?
- Q2 Does every message include a simple opt-out that works?
- Q3 Are opt-outs applied across all systems (DMS, CRM, email tool) promptly?

WHAT NON-COMPLIANCE COSTS YOU

THE FINE

Up to **£17.5 million or 4% of global annual turnover**, whichever is higher. Since **5 Feb 2026**, PECR breaches (marketing and cookies) carry the same ceiling, up from £500,000.

BEYOND THE FINE

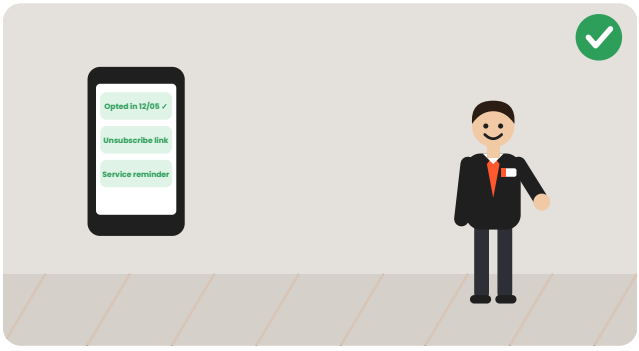
The ICO can issue **enforcement notices** stopping processing or marketing, publish reprimands, and executes **search warrants**. Customers can also claim compensation.

REAL ENFORCEMENT

£60K

ICO fine on **Finance Giant**, a car-sales finance firm, for marketing texts and emails sent without valid consent (2022).

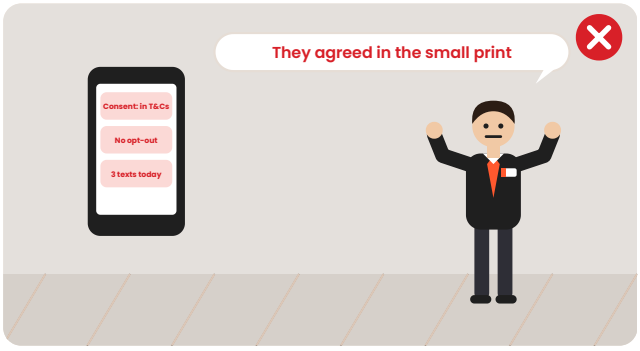
✔ RIGHT WAY



Separate opt-in and an unsubscribe in every message.

✖ WRONG WAY

£17.5M / 4%



Consent buried in T&Cs, no opt-out.

PURPOSE

Car finance marketing is the ICO's top complaint area. Consent forced through terms is exactly what got a car-finance firm fined.

FIX IT WITHIN

Immediate

AUDIT CRITERIA · PASS WHEN

- Separate, unticked consent
- Opt-out in every message
- Opt-outs synced across systems
- Consent records kept

IDEAL WAY OF AUDITING

1. Check the consent form wording
2. Unsubscribe from a test message
3. Trace an opt-out through DMS and CRM

Evidence: Consent records + test results.

WORST CASE Marketing fines were capped at £500,000. Since Feb 2026 they reach **£17.5M or 4% of turnover**.

DAT-02 DATA PROTECTION · ICO · STANDARD 02 OF 07

Cookie Consent

Area **Website · Digital** | Person in charge **Digital Manager** | Regulator **ICO**

MAXIMUM PENALTY

GBP 17.5M

or 4% of global turnover, if higher

Since 5 Feb 2026 the same ceiling applies to **marketing & cookies**

• CRITICAL

THE LAW

UK GDPR

UK GDPR · **Data Protection Act 2018** · **PECR 2003** as amended by the **Data (Use and Access) Act 2025** · **PECR reg.6** cookies and similar technologies (with DUAA exemptions for some analytics)

WHAT WE CHECK

The website asks before setting non-essential cookies (advertising, tracking), with "reject" as easy as "accept", and doesn't fire tags before a choice is made.

CHECKPOINTS IN THE AUDIT

- Q1 Does the cookie banner offer reject as easily as accept?
- Q2 Are advertising and tracking cookies blocked until consent?
- Q3 Is the cookie policy accurate and up to date?

WHAT NON-COMPLIANCE COSTS YOU

THE FINE

Up to **£17.5 million or 4% of global annual turnover**, whichever is higher. Since **5 Feb 2026**, PECR breaches (marketing and cookies) carry the same ceiling, up from £500,000.

BEYOND THE FINE

The ICO can issue **enforcement notices** stopping processing or marketing, publish reprimands, and executes **search warrants**. Customers can also claim compensation.

REAL ENFORCEMENT

35×

increase in the maximum marketing fine: from **£500,000 to £17.5M** when the Data (Use and Access) Act took effect (5 Feb 2026).

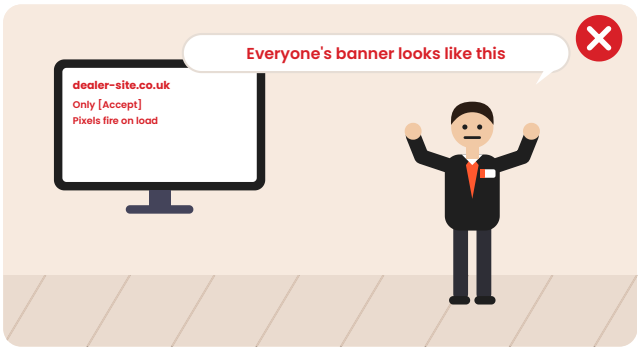
✔ RIGHT WAY



Equal accept and reject; tags wait for consent.

✖ WRONG WAY

£17.5M / 4%



Accept-only banner, trackers firing on load.

PURPOSE

Cookie banners are public, so the ICO can check them from a desk.

FIX IT WITHIN

◷ 7 days

AUDIT CRITERIA · PASS WHEN

- Equal accept and reject
- No tracking before consent
- Accurate policy

IDEAL WAY OF AUDITING

1. Load the site in a clean browser
2. Check which tags fire before a choice
3. Review the policy

Evidence: Browser test + screenshots.

WORST CASE Cookie breaches now fall under the **£17.5M / 4%** ceiling, and every dealer website and portal is visible to the ICO.

DAT-03 DATA PROTECTION · ICO · STANDARD 03 OF 07

Privacy Notice & Lawful Basis

Area **Sales · Service · Website** | Person in charge **DPO · Compliance Officer** | Regulator **ICO**

MAXIMUM PENALTY

GBP 17.5M

or 4% of global turnover, if higher

Since 5 Feb 2026 the same ceiling applies to **marketing & cookies**

• CRITICAL

THE LAW

UK GDPR

UK GDPR · Data Protection Act 2018 · PECR 2003 as amended by the **Data (Use and Access) Act 2025 · UK GDPR Articles 5, 6, 13–14** transparency and lawful basis

WHAT WE CHECK

Customers are told, when data is collected, what's collected, why, the lawful basis, who it's shared with (lenders, OEM, insurers) and how long it's kept.

CHECKPOINTS IN THE AUDIT

- **Q1** Is a privacy notice given at every collection point (showroom, website, service booking)?
- **Q2** Does it name data sharing with lenders, manufacturers and partners?
- **Q3** Is there a documented lawful basis for each use?

WHAT NON-COMPLIANCE COSTS YOU

THE FINE

Up to **£17.5 million or 4% of global annual turnover**, whichever is higher. Since **5 Feb 2026**, PECR breaches (marketing and cookies) carry the same ceiling, up from £500,000.

BEYOND THE FINE

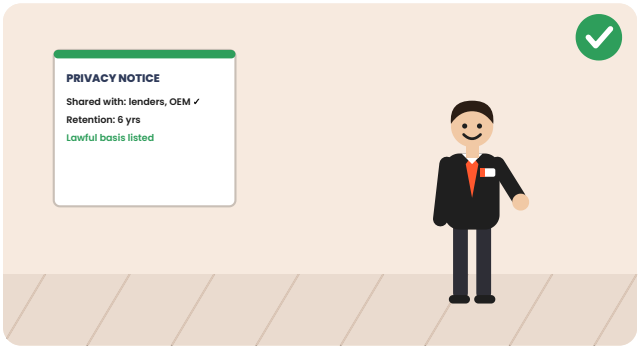
The ICO can issue **enforcement notices** stopping processing or marketing, publish reprimands, and executes **search warrants**. Customers can also claim compensation.

REAL ENFORCEMENT

170M

texts about car finance claims led the ICO to **execute search warrants** in 5 cities (Jul 2026). 12M+ complaints since Sep 2025.

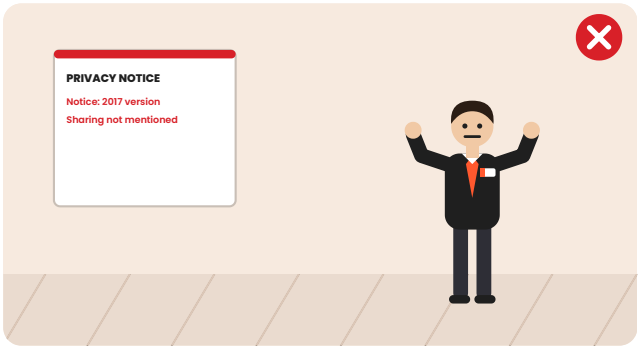
✔ RIGHT WAY



Current notice naming every data share.

✖ WRONG WAY

£17.5M / 4%



A 2017 notice that doesn't mention lenders or the OEM.

PURPOSE

Dealers share data with lenders, manufacturers and telematics partners, and customers must be told.

FIX IT WITHIN

30 days

AUDIT CRITERIA · PASS WHEN

- Notice at every touchpoint
- All sharing named
- Lawful basis documented
- Reviewed yearly

IDEAL WAY OF AUDITING

1. Collect notices from each channel
2. Map data flows
3. Check the record of processing

Evidence: Notices + processing record.

WORST CASE Transparency failures fall in the higher tier: up to **£17.5M or 4% of turnover**.

DAT-04 DATA PROTECTION · ICO · STANDARD 04 OF 07

Subject Access Requests

Area **Customer relations** | Person in charge **DPO** | Regulator **ICO**

MAXIMUM PENALTY

GBP 17.5M

or 4% of global turnover, if higher

Since 5 Feb 2026 the same ceiling applies to **marketing & cookies**

• CRITICAL

THE LAW

UK GDPR

UK GDPR · **Data Protection Act 2018** · **PECR 2003** as amended by the **Data (Use and Access) Act 2025** · **UK GDPR Articles 12 and 15–22** data subject rights

WHAT WE CHECK

Requests for access, correction or deletion are recognised in any form, logged and answered within one month (extendable only where allowed).

CHECKPOINTS IN THE AUDIT

- Q1 Do staff recognise requests however they arrive (email, phone, social media, in person)?
- Q2 Are requests logged and answered within one month?
- Q3 Can the dealer find a customer's data across DMS, CRM, email and call recordings?

WHAT NON-COMPLIANCE COSTS YOU

THE FINE

Up to **£17.5 million or 4% of global annual turnover**, whichever is higher. Since **5 Feb 2026**, PECR breaches (marketing and cookies) carry the same ceiling, up from £500,000.

BEYOND THE FINE

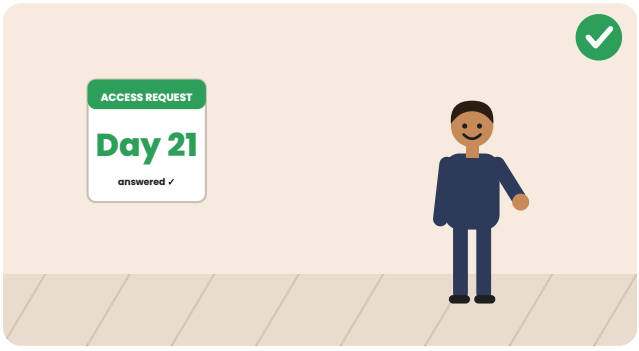
The ICO can issue **enforcement notices** stopping processing or marketing, publish reprimands, and executes **search warrants**. Customers can also claim compensation.

REAL ENFORCEMENT

170M

texts about car finance claims led the ICO to **execute search warrants** in 5 cities (Jul 2026). 12M+ complaints since Sep 2025.

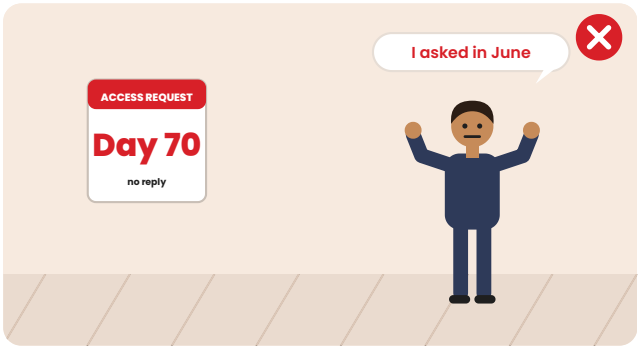
✔ RIGHT WAY



Answered on day 21.

✖ WRONG WAY

£17.5M / 4%



No reply after 70 days.

PURPOSE

Access requests are rising with car finance claims. Claims firms send them in bulk.

FIX IT WITHIN

◷ 7 days

AUDIT CRITERIA · PASS WHEN

- Requests logged
- Answered within 1 month
- Data found across systems
- Staff trained

IDEAL WAY OF AUDITING

1. Review the request log
2. Time 5 recent requests
3. Test a search across systems

Evidence: Request log.

WORST CASE Missed deadlines lead to ICO complaints and **enforcement notices**, with fines up to £17.5M.

DAT-05 DATA PROTECTION · ICO · STANDARD 05 OF 07

Security & Breach Reporting

Area **Showroom · IT** | Person in charge **IT Manager · DPO** | Regulator **ICO**

MAXIMUM PENALTY

GBP 8.7M

or 2% of global turnover, if higher

Plus **customer compensation claims** after a breach

• CRITICAL

THE LAW

UK GDPR

UK GDPR · Data Protection Act 2018 · PECR 2003 as amended by the **Data (Use and Access) Act 2025 · UK GDPR Articles 32–34** security of processing and personal data breach notification

WHAT WE CHECK

Customer data is protected (access control, MFA, encryption, locked paper files), and breaches are reported to the ICO within 72 hours where required.

CHECKPOINTS IN THE AUDIT

- **Q1** Are DMS, CRM and email protected by strong access control and multi-factor authentication?
- **Q2** Are paper deal files locked away and shredded when no longer needed?
- **Q3** Is there a breach procedure with the 72-hour ICO deadline?

WHAT NON-COMPLIANCE COSTS YOU

THE FINE

Up to **£17.5 million or 4% of global annual turnover**, whichever is higher. Since **5 Feb 2026**, PECR breaches (marketing and cookies) carry the same ceiling, up from £500,000.

BEYOND THE FINE

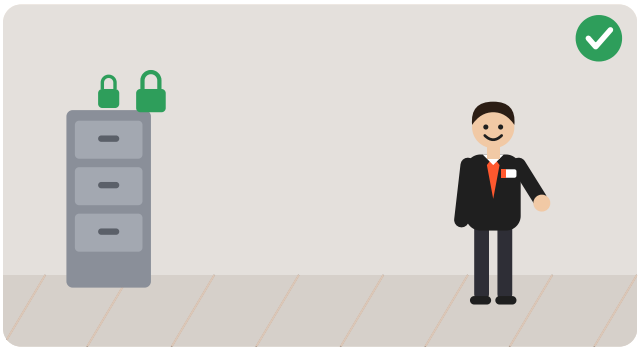
The ICO can issue **enforcement notices** stopping processing or marketing, publish reprimands, and executes **search warrants**. Customers can also claim compensation.

REAL ENFORCEMENT

£225K

in ICO fines announced in Jan 2026 for **nuisance marketing messages**.

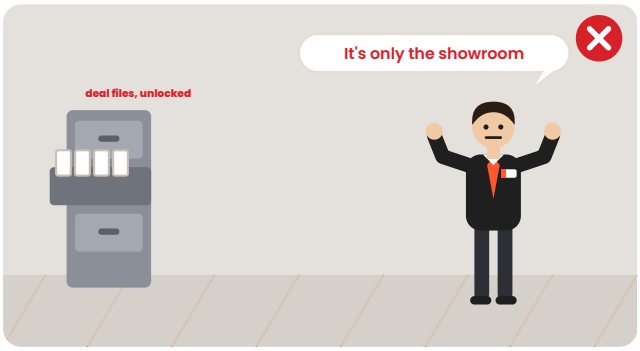
✔ RIGHT WAY



Deal files locked, MFA on systems.

✖ WRONG WAY

£8.7M / 2%



Open cabinet of deal files with driving licences.

PURPOSE

Deal files hold licences, bank details and payslips: exactly what fraudsters want.

FIX IT WITHIN

24 hours

AUDIT CRITERIA · PASS WHEN

- MFA on key systems
- Paper locked and shredded
- Breach procedure
- 72-hour reporting known

IDEAL WAY OF AUDITING

1. Check MFA settings
2. Walk the showroom for files
3. Ask who reports a breach

Evidence: Settings + photos + procedure.

WORST CASE Poor security is fined in the lower tier (up to **£8.7M or 2%**), and a breach brings customer claims on top.

DAT-06 DATA PROTECTION · ICO · STANDARD 06 OF 07

Retention & Disposal

Area **All departments** | Person in charge **DPO** | Regulator **ICO**

MAXIMUM PENALTY

GBP 17.5M

or 4% of global turnover, if higher

Since 5 Feb 2026 the same ceiling applies to **marketing & cookies**

• CRITICAL

THE LAW

UK GDPR

UK GDPR · **Data Protection Act 2018** · **PECR 2003** as amended by the **Data (Use and Access) Act 2025** · **UK GDPR Article 5(1)(e)** storage limitation

WHAT WE CHECK

There's a retention schedule for sales, finance, service and marketing data, and old records are deleted or shredded on schedule.

CHECKPOINTS IN THE AUDIT

- Q1 Is there a written retention schedule by record type?
- Q2 Are old records deleted from systems and shredded on paper?
- Q3 Is disposal logged, including by third-party shredders?

WHAT NON-COMPLIANCE COSTS YOU

THE FINE

Up to **£17.5 million or 4% of global annual turnover**, whichever is higher. Since **5 Feb 2026**, PECR breaches (marketing and cookies) carry the same ceiling, up from £500,000.

BEYOND THE FINE

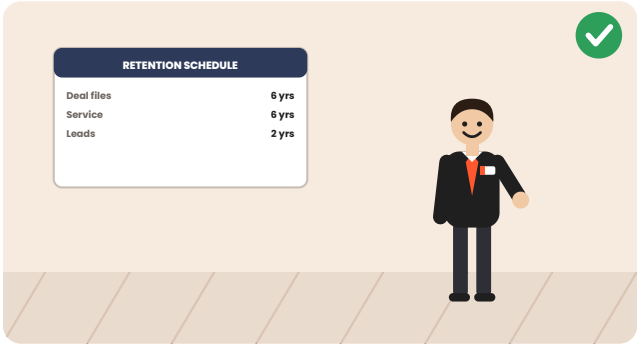
The ICO can issue **enforcement notices** stopping processing or marketing, publish reprimands, and executes **search warrants**. Customers can also claim compensation.

REAL ENFORCEMENT

170M

texts about car finance claims led the ICO to **execute search warrants** in 5 cities (Jul 2026). 12M+ complaints since Sep 2025.

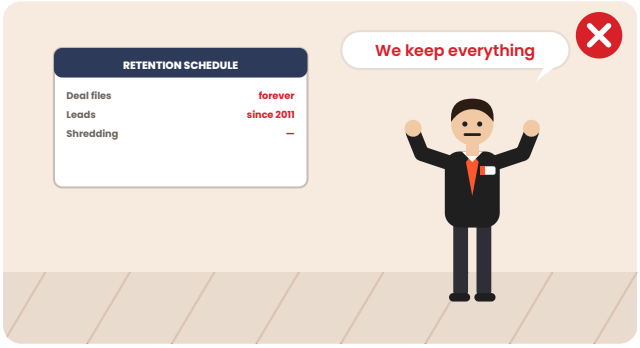
✔ RIGHT WAY



Retention periods set and followed.

✖ WRONG WAY

£17.5M / 4%



Leads kept since 2011.

PURPOSE

Old data is risk with no value: it can only be breached or misused.

FIX IT WITHIN

30 days

AUDIT CRITERIA · PASS WHEN

- Schedule approved
- Deletion routines running
- Shredding certificates

IDEAL WAY OF AUDITING

1. Request the schedule
2. Check the oldest records in the CRM
3. Check shredding certificates

Evidence: Schedule + certificates.

WORST CASE Keeping data too long is a principle breach in the **higher tier**: up to £17.5M or 4%.

DAT-07 DATA PROTECTION · ICO · STANDARD 07 OF 07

ICO Fee Paid

Area **Finance · Compliance** | Person in charge **Finance Director** | Regulator **ICO**

MAXIMUM PENALTY

GBP 4,350

maximum fixed penalty for not paying

And it flags the business for **further scrutiny**

• MODERATE

THE LAW

UK GDPR

UK GDPR · Data Protection Act 2018 · PECR 2003 as amended by the **Data (Use and Access) Act 2025 · Data Protection (Charges and Information) Regulations 2018**

WHAT WE CHECK

The dealership (each legal entity) pays the annual data protection fee to the ICO and keeps its registration details up to date.

CHECKPOINTS IN THE AUDIT

- Q1 Has every legal entity in the group paid the ICO data protection fee?
- Q2 Are the registration details (address, DPO contact) current?

WHAT NON-COMPLIANCE COSTS YOU

THE FINE

Up to **£17.5 million or 4% of global annual turnover**, whichever is higher. Since **5 Feb 2026**, PECR breaches (marketing and cookies) carry the same ceiling, up from £500,000.

BEYOND THE FINE

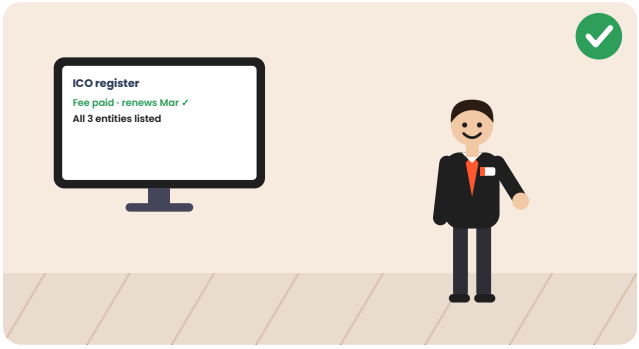
The ICO can issue **enforcement notices** stopping processing or marketing, publish reprimands, and executes **search warrants**. Customers can also claim compensation.

REAL ENFORCEMENT

£225K

in ICO fines announced in Jan 2026 for **nuisance marketing messages**.

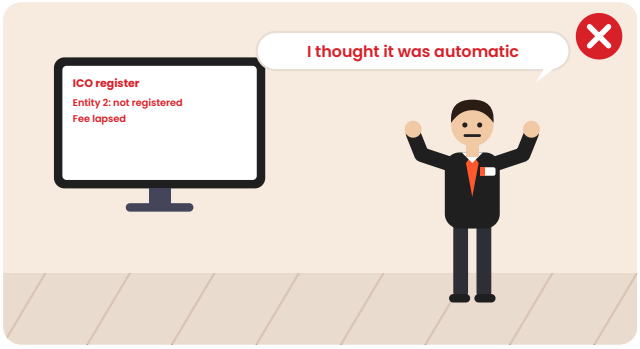
✔ RIGHT WAY



Fee paid for every entity.

✖ WRONG WAY

£4,350



One entity never registered.

PURPOSE

The easiest check the ICO can do, and a fixed penalty if missed.

FIX IT WITHIN

◷ 7 days

AUDIT CRITERIA · PASS WHEN

- All entities registered
- Fee current
- Details correct

IDEAL WAY OF AUDITING

1. Search the ICO register
2. Compare with Companies House

Evidence: Register screenshots.

WORST CASE Not paying the fee is a **fixed penalty up to £4,350**, and puts the business on the ICO's radar.

FIX CONSENT BEFORE THE NEXT CAMPAIGN

Your 30-day data action plan.

Today

- [ ] **DAT-01** Marketing Consent
  ◷ Immediate
- [ ] **DAT-05** Security & Breach Reporting
  ◷ 24 hours

This week

- [ ] **DAT-02** Cookie Consent
  ◷ 7 days
- [ ] **DAT-04** Subject Access Requests
  ◷ 7 days
- [ ] **DAT-07** ICO Fee Paid
  ◷ 7 days

This month

- [ ] **DAT-03** Privacy Notice & Lawful Basis
  ◷ 30 days
- [ ] **DAT-06** Retention & Disposal
  ◷ 30 days

?/7 Count your passes. Marketing and cookie fails now sit under the **£17.5M / 4%** ceiling.

SOURCES

- ICO: Multiple properties searched after millions of car finance complaints (Jul 2026) · ico.org.uk
- Clifford Chance: Key aspects of the Data (Use and Access) Act take effect (Feb 2026) · cliffordchance.com
- Decision Marketing: Car finance firm fined for illegal texts (Finance Giant, 2022) · decisionmarketing.co.uk
- ICO: Fines of £225,000 for nuisance marketing messages (Jan 2026) · ico.org.uk
- UK GDPR; Data Protection Act 2018; PECR 2003; Data (Use and Access) Act 2025 · legislation.gov.uk

Disclaimer. For compliance-audit guidance only; not legal advice. Maximum fines shown. Some DUAA changes (e.g. cookie exemptions) have detailed conditions; check current ICO guidance.

AUDIT SIGN-OFF

DEALERSHIP / SITE	AUDITOR	DATE	SCORE __ / 7

BRANCH / DEALER PRINCIPAL SIGNATURE	COMPLIANCE LEAD SIGNATURE