A PERSONAL DATA CHECKLIST FOR COMPANIES

Delete by default

Keep what you need, for as long as you need it. Delete everything else.

Every piece of personal data you hold is something you have to protect, and something that can hurt the person it belongs to if it leaks. The safest data is data you never collected, and the next safest is data you've already deleted. This checklist is built on UK GDPR, ICO guidance, the OWASP Top 10 Privacy Risks and PCI DSS. The source for each item is underneath it.

1. Collect less

- [ ] Every field has a written reason. No reason, no field.
  UK GDPR Art. 5(1)(b)-(c). ICO: data minimisation.
- [ ] Collect the smallest version that answers the question: an age band, not a birthday. The first half of a postcode, not the address. A month, not a date.
  ICO: data protection by design and by default.
- [ ] Don't collect anything “in case”. If you need it later, ask later.
  OWASP Top 10 Privacy Risks, P10.
- [ ] Optional fields are genuinely optional, and saying no doesn't block the service.

2. Keep it for less time

- [ ] Every data set has an owner and a written retention period.
  UK GDPR Art. 5(1)(e). ICO: storage limitation.
- [ ] Deletion runs automatically. It isn't a task someone has to remember.
  OWASP Top 10 Privacy Risks, P6.
- [ ] ID scans, selfies and source documents are deleted as soon as the check is done.
- [ ] Retention covers everything: backups, logs, exports, spreadsheets, inboxes, support tickets and analytics.
- [ ] Where the law says keep it, write down the rule, keep only what it requires, and delete on the day it expires.
  ICO: storage limitation.

3. Store it carefully

- [ ] Personal data is encrypted in transit and at rest.
  UK GDPR Art. 32.
- [ ] Only the people who need it can see it, and access is reviewed regularly.
- [ ] Personal data never lives in spreadsheets, email attachments or chat threads.
- [ ] Card security codes are never stored after authorisation. Paper counts.
  PCI DSS Requirement 3.

4. Share less

- [ ] Every supplier that touches personal data has a contract requiring it to delete or return the data when the work ends. You check that it does.
  UK GDPR Art. 28. ICO: controller and processor contracts.
- [ ] Outsourcing a task doesn't outsource the responsibility.

- [ ] Requests for personal data are verified through a contact route you already hold, never through the one the request arrived on.
- [ ] Data is aggregated or de-identified before it leaves the building.

5. Measure without hoarding

- [ ] Count, don't record. Increment a total instead of storing a row per person.
- [ ] Roll raw events up into totals, then delete the raw events.
- [ ] Use identifiers that expire, so you can count visitors without following anyone.
- [ ] Model training and “future analytics” aren't a reason to keep personal data.
  UK GDPR Art. 5(1)(b).

6. Be ready

- [ ] You have an up-to-date list of what personal data you hold, where, why and for how long.
  UK GDPR Art. 30.
- [ ] You have a breach plan and have practised it. Reportable breaches go to the regulator within 72 hours.
  UK GDPR Art. 33. ICO: 72 hours.
- [ ] You test deletion like you test backups: pick a record and prove it's gone everywhere.

> **The test: if you were breached tonight, what would you wish you hadn't kept? Delete it tomorrow.**

Sources

UK GDPR, Article 5 (principles), 25, 28, 30, 32 and 33. legislation.gov.uk/eur/2016/679

ICO: Data minimisation. ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/data-minimisation/

ICO: Storage limitation. ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/storage-limitation/

ICO: Data protection by design and by default. ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-by-design-and-by-default/

ICO: What needs to be included in the contract (controllers and processors). ico.org.uk

ICO: 72 hours, how to respond to a personal data breach. ico.org.uk

OWASP Top 10 Privacy Risks, v2.0. owasp.org/www-project-top-10-privacy-risks/

PCI Security Standards Council: card verification codes must not be stored after authorization. blog.pcisecuritystandards.org

This is a practical checklist, not legal advice. Check the rules that apply to you where you operate.