OWNER CHECKLIST · KSA · UAE · EGYPT

Data Protection for Your Finance Function

A practical checklist for owners: what personal data finance holds, who can see it, how long you keep it, what to demand from vendors, and what to do in a breach.

Not legal advice. This checklist is general operational guidance. Laws and regulations change, and how they apply depends on your facts. Before relying on it, confirm the current rules with the regulator and a lawyer licensed in your country. Legal references were checked against official or primary sources on 4 November 2026 (see Sources, last page).

How to use this checklist (about 60 minutes)

Step	What to do	Where
1	Confirm which data protection law(s) apply to you.	Section 1
2	List the personal data your finance team holds and where it sits.	Section 2
3	Tick the access, retention and vendor controls you already have. Every empty box is an action.	Sections 3–5
4	Fill in the breach contact sheet and keep it where two people can find it.	Section 6
5	Review once a year, and whenever you change accounting system, payroll provider or outsourced accountant.	—

1. Which law applies to you?

Each law applies to personal data about individuals (employees, customers who are individuals, sole-trader suppliers, guarantors). It does not cover purely company data, but a finance function holds a lot of personal data. If you operate in more than one country, more than one law can apply.

	Saudi Arabia	UAE (federal)	Egypt
Law	Personal Data Protection Law (PDPL), Royal Decree M/19 (9/2/1443H), amended by Royal Decree M/148 (5/9/1444H), plus its Implementing Regulation.	Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data. Issued 20 Sep 2021; in force 2 Jan 2022.	Personal Data Protection Law No. 151 of 2020, plus Executive Regulations issued by Ministerial Decree No. 816 of 2025 (Official Gazette, 1 Nov 2025).
Regulator	Saudi Data & AI Authority (SDAIA).	The federal data regulator named in the law (UAE Data Office). Check u.ae for the current authority.	Personal Data Protection Center (PDPC).
Breach: who tells the regulator, and when	Controller notifies SDAIA within 72 hours of becoming aware, where the breach may harm the data or the individuals (Implementing Reg. Art. 24).	Controller notifies the regulator on becoming aware, within the period set by the Executive Regulations (Art. 9). Check whether these have been issued.	Controller and processor notify the PDPC within 72 hours of becoming aware (Exec. Regs Art. 5).
Breach: telling affected people	Without undue delay, where the breach may cause damage or affect their rights (Art. 24(5)).	Where the breach affects their privacy, within the period set by the Executive Regulations (Art. 9(2)).	Within 3 working days of notifying the PDPC (Exec. Regs Art. 5).
Your vendor (processor) must tell you	Without undue delay; this must be written into the contract (Implementing Reg. Art. 17).	As soon as it becomes aware (Art. 9(3)).	The processor also reports directly to the PDPC (see above). Agree in the contract that it tells you at the same time.

	Saudi Arabia	UAE (federal)	Egypt
Key points to check	Fines: warning or up to SAR 5 million per violation, doubled for repeat violations (PDPL Art. 36). Disclosing sensitive data to cause harm or for personal benefit: up to 2 years' prison and/or SAR 3 million (Art. 35). SDAIA opened a consultation on amendments to the Implementing Regulation in October 2026: check for the final text.	Does not apply to companies in free zones with their own data protection law (e.g. DIFC, ADGM), or to health and banking/credit data covered by their own legislation (Art. 2). The fines schedule is left to a Cabinet decision (Art. 26).	Controllers and processors may need a licence or permit from the PDPC and a registered Data Protection Officer. The one-year adjustment period after the Executive Regulations is widely read as ending 1 Nov 2026: confirm your status with the PDPC.

My company is a ☐ Controller (we decide why and how the data is used) ☐ Processor (we handle it for a client) ☐ Both

Laws that apply to us: ☐ KSA PDPL ☐ UAE federal PDPL ☐ DIFC / ADGM law ☐ Egypt PDPL ☐ Other: _____

2. What personal data does your finance team hold?

Fill in the last three columns. The examples show what most SMEs hold; delete rows that do not apply and add any that are missing. Rows marked **Sensitive** need extra care: limit access to the fewest people possible.

Data held	About whom	Where it sits (system / folder)	Who can access	Keep until
Payroll: salaries, allowances, deductions, bank IBANs	Employees			
ID and residency documents (national ID, Iqama, Emirates ID, passport copies)	Employees, guarantors			
Medical certificates, sick-leave notes, insurance claims attached to expenses	Employees — **Sensitive**			
End-of-service, loans and advances to staff	Employees			
Customer billing details, e-invoices with individual buyers' names	Customers who are individuals			
Credit checks, payment history, collection notes	Customers, guarantors			
Supplier bank details for sole traders and freelancers	Individual suppliers			
Owner / shareholder personal data held for banks, auditors, KYC	Owners, directors			
Bank statements and card statements showing individual payees	Employees, customers, suppliers			
Other: _____				

3. Access control checklist

Tick what is true today. Every empty box is an action for this month.

	Control	Owner / due date
☐	**Named users only.** No shared logins to the accounting system, bank portal or payroll.	
☐	**Multi-factor authentication** on accounting, payroll, banking, email and cloud storage.	

	Control	Owner / due date
☐	**Role-based access.** Payroll and HR files visible only to the people who run payroll.	
☐	**Bank approvals split:** the person who creates a payment is not the person who approves it.	
☐	**Joiner / leaver process:** access removed on the last working day, including vendor staff.	
☐	**Quarterly access review:** print the user list for each system and confirm every name.	
☐	**No personal email or messaging apps** for payroll files, ID copies or bank details.	
☐	**Encrypted laptops and phones** for anyone who opens finance files; screen lock on.	
☐	**Activity logs switched on** in the accounting system and someone knows how to export them.	
☐	**Backups tested:** you have restored a file in the last 6 months.	

4. Retention and destruction

The data protection laws say: keep personal data only as long as you need it, unless another law requires you to keep it longer, then destroy it securely. For example, Saudi PDPL Art. 18 requires destruction once the purpose ends, but retention where there is a legal basis for a specific period. Tax, commercial and labour laws set minimum record-keeping periods for finance records.

> **Do not guess the periods.** Enter the minimum period from your tax authority (ZATCA, UAE FTA, Egyptian Tax Authority), commercial law and labour law, and note where you found it. Your auditor or tax adviser can confirm.

Record type	Legal minimum (enter + source)	Our rule	Destroy how / who
Accounting books, ledgers, invoices			
VAT / tax returns and supporting records			
Payroll and employee files (after leaving)			
ID and passport copies			
Customer credit and collection files			
Bank statements			

- Destruction covers every copy: email attachments, shared drives, laptops, backups and the vendor's systems.
- Keep a short destruction log (date, record type, method, who approved).

5. Vendors who touch your finance data

Outsourced accountants, payroll bureaus, cloud accounting software, banks' cash-management portals, auditors and IT support may all process personal data for you. Under the Saudi PDPL you must choose processors that give sufficient guarantees and monitor them (PDPL Art. 8); the Implementing Regulation (Art. 17) lists what the contract must contain. Use this list for every vendor.

5a. Contract clauses to look for

	Clause	Why
☐	Purpose, categories of personal data and duration of processing are written down.	Required in KSA (Impl. Reg. Art. 17).
☐	Vendor processes only on your written instructions; tells you in writing if an instruction would break the law.	KSA Art. 17(2); good practice everywhere.
☐	Vendor tells you about any breach without undue delay (agree a number of hours).	KSA Art. 17; UAE Art. 9(3).
☐	Sub-processors named; no new ones without notice and a chance to object.	KSA Art. 17(5).
☐	Vendor states whether foreign laws apply to it, and where the data is stored.	KSA Art. 17(1)(e); cross-border rules (KSA Art. 29; Egypt licence).
☐	Security measures described: access control, MFA, encryption, logging, backups.	All three laws require appropriate security.
☐	Your right to audit or receive an independent assurance report.	Lets you monitor the processor.
☐	Exit: data returned in a usable format, then deleted, with written confirmation.	Avoids lock-in and leftover copies.
☐	No right to withhold your data in a fee dispute.	Protects continuity.
☐	Confidentiality continues after the contract ends.	KSA PDPL Art. 41.

5b. Vendor register

Vendor	What data	Contract with data clauses?	Data stored in (country)	Last reviewed

Tip: Where you can, keep the accounting system on your own subscription and give vendor staff named user accounts. You keep the data, see the activity log, and can remove access in minutes if the relationship ends.

6. Breach response: first 72 hours

A breach is any incident that exposes, alters, destroys or gives unauthorised access to personal data, e.g. a payroll file emailed to the wrong person, a stolen laptop, a hacked email account, or a vendor incident.

When	Action	Done
Hour 0–2	Contain: reset passwords, revoke access, recall emails, isolate devices. Write down the time you became aware.	☐
Hour 2–12	Assess: what data, how many people, which countries, is it sensitive (IDs, health, bank details)? Ask the vendor for its incident report.	☐
Hour 12–24	Decide with your lawyer whether the legal threshold for notifying the regulator and individuals is met in each country.	☐
By hour 72	KSA: notify SDAIA (where the breach may cause harm). Egypt: notify the PDPC. UAE: follow the Executive Regulations once issued; record your decision either way.	☐
Next days	Tell affected individuals where required (KSA: without undue delay; Egypt: within 3 working days of notifying the PDPC). Use simple language and say what they should do.	☐

When	Action	Done
Within 30 days	Fix the root cause, keep copies of all notices and evidence, and update this checklist.	☐

Breach contact sheet (fill in now)

Role	Name	Phone	Email
Breach lead (decides and coordinates)			
IT / system administrator			
Data protection officer (if appointed)			
External lawyer			
Outsourced accountant / payroll vendor			
Regulator portal / hotline (from the regulator's website)			

7. Ten questions to ask an outsourced accountant or payroll provider

- ☐ Which named people will access our data, and how are they vetted and bound to confidentiality?
- ☐ Will you work inside our accounting system, or will our data sit in yours?
- ☐ Where is the data stored, and is any of it transferred or accessible outside the country?
- ☐ Who are your sub-processors (cloud, software, freelancers)? Show us the list.
- ☐ Can we see your standard data processing terms, and will you accept our changes?
- ☐ How quickly will you tell us about a breach, and who will call us?
- ☐ Do you use MFA, encrypted devices and named logins for all staff?
- ☐ Do you hold any licence, registration or certification required for processors in our country?
- ☐ If we end the contract, how and when do we get our data back, and how do you confirm deletion?
- ☐ Have you had a security incident in the last two years, and what did you change afterwards?

If a provider cannot answer most of these clearly and in writing, treat it as a warning sign.

Sources checked on 4 November 2026

Official texts are listed first. Secondary sources were used only to confirm status where the official portal could not be read directly; confirm before relying on them.

Saudi PDPL (amended), official English translation, SDAIA: sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf (Arts. 8, 18, 29, 35, 36, 41).

Saudi PDPL Implementing Regulation, SDAIA: sdaia.gov.sa/en/SDAIA/about/Documents/ImplementingRegulation.pdf (Arts. 17, 23, 24, 32, 33).

SDAIA consultation on draft amendments to the Implementing Regulation (Oct 2026), reported by Al Tamimi & Co.: tamimi.com/news/sdaia-opens-public-consultation-on-proposed-amendments-to-the-pdpl-implementing-regulation/

UAE Federal Decree-Law No. 45 of 2021, UAE Legislation portal: uaelegislation.gov.ae/en/legislations/1972 (issue and effective dates; Arts. 2, 9, 26).

UAE Executive Regulations status: not found on the portal; secondary reports dated Sep–Oct 2026 state they remain outstanding, e.g. itsecnow.com/post/uae-pdpl-in-2026-the-executive-regulations-still-arent-issued-heres-what-applies-today

Egypt Executive Regulations, Ministerial Decree No. 816 of 2025, Official Gazette No. 244 (Supp. A), 1 Nov 2025, English translation: thesedonaconference.org (meeting paper 7.4) and shehatalaw.com translation (Art. 5 breach notification).

Egypt adjustment period and licensing summary, Baker McKenzie (Jan 2026): bakermckenzie.com – "Egypt: Important Data Protection Update".

ملخص بالعربية

حماية البيانات في الإدارة المالية — قائمة تحقق لصاحب المنشأة

هذه القائمة إرشادات عملية عامة وليست استشارة قانونية. تأكّد من القواعد الحالية مع الجهة الرقابية ومحامٍ مرخّص في بلدك. تمت مراجعة المراجع القانونية بتاريخ 4 نوفمبر 2026.

1. حدّد القانون المطبّق: نظام حماية البيانات الشخصية السعودي (سدايا)، المرسوم بقانون اتحادي رقم 45 لسنة 2021 في الإمارات، أو القانون المصري رقم 151 لسنة 2020 ولائحته التنفيذية (الجهة: مركز حماية البيانات الشخصية).
2. اعمل جرداً للبيانات الشخصية لدى الإدارة المالية: الرواتب والحسابات البنكية للموظفين، صور الهويات والإقامات، التقارير الطبية، بيانات العملاء الأفراد والموردين الأفراد.
3. ضوابط الوصول: مستخدمون بأسماء محددة، تحقق متعدد العوامل، صلاحيات حسب الدور، وإلغاء الوصول فور انتهاء العمل.
4. مدة الاحتفاظ: أدخل الحد الأدنى المطلوب من مصلحة الضرائب والأنظمة التجارية ونظام العمل في بلدك، ثم أتلف البيانات بشكل آمن.
5. المورّدون: عقد يحدد الغرض وفئات البيانات والمدة، والإبلاغ عن الاختراق دون تأخير، والإفصاح عن المعالجين الفرعيين، وإعادة البيانات وحذفها عند الخروج.
6. الاختراق: في السعودية يُبلَّغ سدايا خلال 72 ساعة إذا كان قد يُلحق ضرراً، وفي مصر يُبلَّغ المركز خلال 72 ساعة وصاحب البيانات خلال 3 أيام عمل. جهّز قائمة جهات الاتصال الآن.

Axcell Financial Consulting · axcellservice.com · Free template · Book a free 30-minute consultation: axcellservice.com/contact