FREE OPERATIONAL RESOURCE

The UAE SME Data Protection Blueprint

A no-fluff operational manual: translate Federal Decree-Law No. 45 of 2021 into ready-to-use RoPA schemas, vendor review checklists and breach response workflows.

WHAT IS INSIDE

✓	**Article 7/8 RoPA structure:** controller and processor record schemas with worked examples
✓	**Third-party DPA clause checklist:** vendor review, clause list and provider-type notes for cloud, payments, e-commerce and local IT providers
✓	**72-hour breach triage matrix:** classification rubric, internal timeline and notification checklist
✓	**Bilingual consent copy blocks:** Arabic and English scripts for checkouts, forms, WhatsApp and cookies

PDF Document (print and digital) | 14 pages | 100% free

Version 1.0 | September 2026 | fyrahprivacy.com

FyrahPrivacy is a specialized data privacy engineering and compliance consultancy practice, not a licensed UAE law firm. This blueprint is general operational guidance, not legal advice. Article references are working references: verify them against the official text before relying on them.

Start Here: How to Use This Blueprint

A no-fluff operating manual for UAE SMEs. Fill it in, hand it to your team, and keep it current.

Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (UAE PDPL) applies to how your business collects, uses, shares, stores and deletes personal data. This blueprint turns that duty into four working tools you can use this week: a records-of-processing schema, a vendor and DPA checklist, a breach triage matrix, and bilingual consent copy.

How to use it

1. Read page 3 to confirm the PDPL applies and whether you act as controller, processor, or both.
2. Build your record of processing using the schema on pages 4 and 5.
3. Review every vendor that touches personal data using pages 6 to 8.
4. Agree your breach response with the team using pages 9 and 10 before an incident happens.
5. Replace consent wording on forms, checkouts and WhatsApp campaigns using pages 11 and 12.
6. Work through the 30-day plan and self-check on page 13.

READ THIS FIRST: LEGAL STATUS OF THIS DOCUMENT

- **Not legal advice.** FyrahPrivacy is a data privacy engineering and compliance consultancy, not a law firm. Use this blueprint as an operational starting point and take legal advice on contract or enforcement questions.
- **Article numbers are working references** to the structure of the PDPL (for example Articles 7 and 8 for controller and processor duties, Article 9 for breach reporting). Check them against the official text before quoting them externally.
- **Executive Regulations.** Many details (timing, procedures, penalties) are left to regulations or Cabinet decisions. Reliable sources reviewed in 2026 still described the Executive Regulations as not yet issued. Where this blueprint gives a time target (for example 72 hours for breach preparation), it is an **internal working target**, not a statutory deadline. Always confirm the position in force.
- **Arabic wording** is a working draft. Have a qualified Arabic legal-terminology reviewer confirm it before you publish it.

What is inside

Tool	What you get	Pages
Applicability check	Does the PDPL apply, and what is your role	3
Article 7/8 RoPA structure	Controller and processor record schemas with worked examples	4 to 5
Third-party review and DPA checklist	Vendor due diligence, clause checklist, provider-type notes	6 to 8
Breach triage matrix	Classification rubric, 72-hour internal workflow, notification checklist	9 to 10
Bilingual consent copy blocks	English and Arabic scripts for checkouts, forms, WhatsApp, cookies	11 to 12
30-day action plan and self-check	Week-by-week plan and 15-point readiness check	13
Glossary, sources, next steps	Terms, where to verify, how FyrahPrivacy can help	14

1. Does the PDPL Apply, and What Is Your Role?

Answer these five questions in ten minutes. Write the answers down: they become the first page of your compliance file.

#	Question	If the answer is YES	Your answer
1	Do we collect or use personal data of individuals in the UAE (customers, leads, staff, visitors)?	The PDPL is likely relevant. Continue.	☐ Yes ☐ No
2	Are we licensed on the UAE mainland, or in a free zone that has no data-protection law of its own?	The PDPL is presumed to apply. Confirm free-zone status with the zone authority.	☐ Yes ☐ No
3	Are we licensed in DIFC or ADGM?	Those zones have their own regimes (DIFC Data Protection Law No. 5 of 2020; ADGM Data Protection Regulations 2021). Take advice on which law applies to which entity.	☐ Yes ☐ No
4	Do we hold health data, or banking and credit data?	The PDPL excludes data governed by sector legislation. Identify the sector regulator and its rules as well.	☐ Yes ☐ No
5	Do we send personal data to vendors or systems outside the UAE (cloud, SaaS, support)?	Cross-border transfer rules apply (working reference Articles 22 and 23). Record every transfer.	☐ Yes ☐ No

Controller or processor?

Your role decides which duties you carry. Many SMEs are **both**: a controller for their own customers and staff, and a processor when they handle data on behalf of a client.

	Controller	Processor
Decides	Why and how personal data is used	Nothing about purpose: acts on the controller's written instructions
Typical SME examples	Online shop handling its own customers; employer handling payroll; marketing list owner	Agency, IT provider, SaaS vendor or accountant handling data for a client
Core duties (Art. 7 / Art. 8)	Lawful ground, transparency, security, records, rights handling, breach reporting, vendor contracts	Process only on instructions, keep a record, secure the data, help the controller, report incidents to the controller
Record to keep	Controller record (page 4)	Processor record (page 5)

LAWFUL GROUND IN ONE LINE

The PDPL is consent-first. Article 4 lists the cases where personal data may be processed without consent, for example where needed to perform a contract or to comply with a legal obligation. Record which ground you rely on for each activity, and do not describe a ground as "legitimate interest": practitioners note the PDPL has no general basis of that name.

2. Article 7/8 RoPA Structure: Controller Record

One row per processing activity (for example "process online orders"), not per system. Articles 7 and 8 set the duty to keep a record; this schema covers the fields good practice and likely regulations expect.

Field	What to record	Example
Ref	Stable ID, never reused	RoPA-001
Department and owner	Function and named person who confirms accuracy	Sales, Head of Sales
Processing activity	Verb-led name	Process online orders
Purpose(s)	Specific purposes. Avoid "business operations"	Fulfil and deliver customer orders; issue invoices
Data subjects	Whose data	Customers
Personal data categories	List fields, not just categories	Name, phone, delivery address, email, order history
Sensitive data?	Yes or no and which kind (health, biometric, financial, children and so on)	No
Lawful ground	Consent, contract, legal obligation or other Article 4 ground, with the article	Contract (Art. 4)
Source	Directly from the person, third party, generated	Directly from the customer
Recipients and processors	Everyone who receives the data	Courier, payment provider, e-commerce platform
Systems and location	Application, database, country or region	Shop platform; hosted in [region]
Cross-border transfer	Yes or no, destination, mechanism, link to your transfer note	Yes: payment provider, [country], contract clauses
Retention	A rule and a trigger, not "as long as needed"	5 years after the last order (accounting records)
Security measures	Encryption, access control, logging, backups	TLS in transit; encryption at rest; role-based access
Impact assessment needed?	Yes, no, or under review (high-risk checks)	No
Where rights requests are served	System to search for access or deletion	Shop platform and email archive
Last reviewed / version	Date and reviewer initials	2026-09-30 / v1.0

3. RoPA Structure: Processor Record and Worked Example

If you handle personal data on behalf of clients, keep a separate processor record (Article 8). Keep one entry per client or per service.

Processor field	What to record
Controller (client) and contact	Legal name, contact, contract reference
Services and processing performed	What you do with the data (hosting, support, analytics, payroll)
Categories of personal data and data subjects	Fields and whose data
Instructions received	Where the written instructions sit (contract, DPA, ticket)
Sub-processors used	Name, country, service, whether the controller approved it
Transfers outside the UAE	Destination, mechanism, controller's authorisation
Security measures	Technical and organisational measures applied
Retention and return or deletion	What happens at contract end, and by when
Incidents	Log of incidents reported to the controller, with dates

Worked example: controller record entry

Ref / activity	RoPA-014 / Send marketing emails to subscribers
Owner	Marketing Manager
Purpose	Send offers and product updates to people who opted in
Data subjects and data	Subscribers: name, email address, language, subscription date and source
Lawful ground	Consent (Art. 4 and Art. 6): separate opt-in, no pre-ticked box
Recipients	Email marketing platform (processor); no other recipients
Transfer	Yes: platform hosted in [country]; contract clauses in place; see transfer note TN-03
Retention	Until consent is withdrawn; inactive for 24 months then review and delete
Security	Platform MFA enforced; export access limited to two named users
Rights handling	Unsubscribe link in every email; erasure requests actioned in the platform within the internal 30-day target

FIVE RULES THAT KEEP A ROPA USEFUL

- Build it from interviews with each department, not from the IT system list alone.
- Reconcile it with your vendor list: every vendor must appear in at least one row.
- Give every row an owner who confirms it once a year.
- Update it when you add a tool, vendor, or marketing channel.
- Store it where your whole team can find it, with a version history.

4. Third-Party Vendor Review Checklist

Run this before you share customer or staff records with any provider (cloud, payments, e-commerce platform, CRM, agency, local IT support). Keep the completed form on file.

#	Check	Evidence to request or record	Done
1	What personal data will the vendor receive, and why?	Data list; purpose; matches your RoPA row	☐
2	Is the vendor a processor, a controller, or both for this use?	DPA or terms stating its role for each purpose	☐
3	Is a signed DPA or processing terms in place?	Signed DPA, or the provider's standard online DPA accepted and saved	☐
4	Where is data stored, and from where can staff access it?	Hosting regions; support locations	☐
5	Does the data leave the UAE, and on what mechanism?	Transfer note with destination and safeguards	☐
6	Which sub-processors does the vendor use, and how are changes notified?	Sub-processor list URL; change-notice route; right to object	☐
7	What security controls protect the data?	Security overview; certifications held (do not assume); MFA, encryption, logging	☐
8	How will the vendor tell you about a breach, and how fast?	Contract clause with a stated notice time	☐
9	Can the vendor help with rights requests and deletion?	Named process or contact; export and delete features	☐
10	What happens to the data when the contract ends?	Return or deletion terms; certificate of deletion	☐
11	Does the vendor use your data to train models or for its own purposes?	Written statement; contract wording	☐
12	Who in your business owns this vendor relationship?	Named owner and next review date	☐

Tier your vendors to focus effort

Tier	Typical vendors	Review depth	Review cycle
1 Critical	Cloud hosting, payments, CRM, e-commerce platform, payroll	Full checklist; signed DPA; transfer note	Annual
2 Significant	Email marketing, support desk, analytics, local IT support	Short checklist; DPA or accepted standard terms	Every two years
3 Low	Tools holding no personal data	Register entry only	On change

5. Third-Party DPA Clause Checklist

Check each clause when a provider sends its DPA, or when you draft your own. Article 8 sets the processor obligations these clauses support.

Clause	What it must say	Red flag
Parties, roles, subject matter	Who is controller, who is processor, what processing the contract covers	Roles unclear or inconsistent across documents
Documented instructions	Processor acts only on the controller's written instructions and tells you if an instruction looks unlawful	Provider may use your data for its own purposes
Data and data subjects	Annex listing data categories and whose data	Blank or generic annex
Confidentiality	Everyone with access is bound by confidentiality	No confidentiality duty on staff or sub-processors
Security measures	Appropriate technical and organisational measures, with minimum controls listed	"Industry standard" with no detail
Sub-processors	Prior authorisation or notice with a right to object; same obligations flowed down; provider liable for them	Unlimited right to change sub-processors with no notice
International transfers	Transfers only to agreed destinations on a stated mechanism	Unrestricted global transfers
Assistance	Help with rights requests, impact assessments, security and breach duties	No assistance commitment
Breach notification	Provider notifies you without undue delay, within a stated number of hours, with defined information	Notice only "as required by law"
Audit and information	You can obtain information or independent audit reports; reasonable on-site right after a serious incident	No information rights
Return or deletion	Data returned or deleted at the end, with confirmation; stated backup tail	Indefinite retention
Liability and indemnity	Allocation reviewed by your counsel	Cap far below the data at risk
Term and termination	DPA runs as long as processing continues; survives termination for deletion	DPA ends before data is deleted
Governing law and language	Law, forum and which language prevails (important if you use an Arabic version)	Silent on language precedence

6. Provider-Type Notes, Transfers and Sub-Processor Register

Use these notes to focus your review. Always read the provider's current documents: terms change.

Provider type	What to check first	Watch for
Cloud infrastructure (for example AWS, Azure, Google Cloud)	Region you actually chose for storage and backups; the provider's standard DPA; sub-processor list; your own access controls (the customer configures most security)	Defaults that place data outside the UAE; shared admin accounts; unchecked backups
Payments (for example Stripe and other gateways)	The role the provider takes for each purpose: providers often act as processor for payment processing and as controller for purposes such as fraud prevention or legal compliance; what data you send; storage of card data	Describing the provider as a processor for everything without reading its terms; card data kept in your own systems
E-commerce and website platforms (for example Shopify)	Standard DPA acceptance; apps and plug-ins you install, each a possible additional vendor; checkout and analytics scripts; customer export and delete tools	Third-party apps with their own data use; marketing pixels firing before consent
Local IT and managed-service providers	A written DPA (rarely offered by default); who has remote or physical access; subcontractors and support from abroad; device and backup handling; return of equipment	Informal arrangements; shared passwords; no confidentiality or breach duty

Cross-border transfer note: five questions

1. What data goes, to which vendor, in which country?
2. Is the destination recognised as providing adequate protection under the rules in force? Record the source and date of your check.
3. If not, which alternative condition applies (for example contractual safeguards) and where is it documented?
4. What technical safeguards reduce risk (encryption, key control, regional hosting)?
5. Who approved the transfer, and when will it be reviewed?

Sub-processor register: columns

Vendor and legal entity	Tier	Service and data	Countries	Transfer mechanism	DPA status	Owner and review date
[Name]	1 / 2 / 3	[What and which data]	[Hosting, support]	[Note ref]	Signed / standard terms / none	[Name, date]

7. Breach Triage Matrix: Classify the Incident

Article 9 (working reference) deals with reporting personal data breaches to the UAE Data Office and, in defined cases, to affected individuals. Timing and procedure may be set by regulations, so confirm the position in force.

ABOUT THE 72-HOUR TARGET

The 72-hour figure used in this blueprint is an **internal working target** for having the notification prepared and decided. It is borrowed from common practice and is **not confirmed as a statutory deadline** under the PDPL. Treat it as a discipline, and check what the law and regulations require at the time of an incident.

Step 1: Is it a personal data breach?

Question	If YES
Is personal data involved (about identifiable people)?	Continue. If no personal data, handle as a security incident.
Was it accessed, disclosed, altered, lost or made unavailable without authorisation?	It is a personal data breach. Open an incident log now (time T0).
Could it prejudice the privacy, confidentiality or security of the personal data?	It is likely reportable to the Data Office. Escalate to the decision-maker immediately.

Step 2: Rate the severity

Level	Criteria (any one is enough)	Typical examples	Response
S1 Critical	Sensitive data or financial credentials; large volume; ongoing exposure; data in criminal hands	Customer database copied; ransomware with data theft; payment data exposed	Activate full team now; executive informed; prepare Data Office notification immediately
S2 High	Ordinary personal data of many people; or suspected sensitive data exposure	Mailing list sent to wrong group; unsecured storage bucket found open	Activate team within hours; contain and assess in parallel; likely notification
S3 Moderate	Limited number of people; contained quickly; low likelihood of harm	One email to wrong recipient, recalled and confirmed deleted	Log; document the decision on notification and the reasons
S4 Low	Near-miss; no personal data exposed	Lost laptop with full-disk encryption and no evidence of access	Log and learn; review controls

8. Breach Workflow: The 72-Hour Internal Timeline

Name an incident lead and a deputy today. Write both phone numbers on this page and store a copy outside your main systems.

Time from awareness (T0)	Action	Owner	Output
T0 to 1 hour	Report to the incident lead; open the incident and decision log; note exact time of discovery	Anyone, then lead	Log opened
1 to 4 hours	Contain: isolate systems, revoke credentials, stop the exposure; preserve evidence (logs, images)	IT lead	Containment note
4 to 24 hours	Assess: which data, how many people, how sensitive, likely harm; assign S1 to S4	Incident lead and privacy owner	Risk assessment
24 to 48 hours	Decide on notification to the Data Office and to individuals; draft notices; get executive approval	Executive decision-maker	Signed decision
By 72 hours (internal target)	Notification prepared and, where required, submitted; processors and key partners informed	Incident lead	Notification copy
After 72 hours	Notify individuals where required; recover; fix root cause; review and update this plan and your RoPA	Whole team	Post-incident report

What a Data Office notification should cover

- ☐ Nature of the breach and when it was discovered
- ☐ Categories and approximate number of people and records affected
- ☐ Likely consequences for those people
- ☐ Measures taken and proposed to contain and reduce harm
- ☐ Name and contact details of the DPO or privacy contact
- ☐ Any processors or other parties involved

Decision log: record every decision

Date and time	Decision	Reason	Decided by

DO AND DO NOT

- **Do** keep facts and opinions separate, and write down times as they happen.
- **Do not** delete evidence, pay or negotiate with attackers without advice, or give informal statements to the media or regulators.
- **Do** test this workflow once a year with a short tabletop exercise.

9. Bilingual Consent Copy Blocks (1): Checkouts and Forms

Replace the bracketed text. Place each block next to the button or field it describes, never inside long terms. Separate marketing consent from order terms.

A. Checkout: order terms (not a consent: the order is processed to perform the contract)

By placing this order you agree to our Terms of Sale. We use your details to process, deliver and invoice your order. See our Privacy Notice [link].

بإتمام هذا الطلب فإنك توافق على شروط البيع لدينا. نستخدم بياناتك لمعالجة طلبك وتسليمه وإصدار فاتورته. راجع إشعار الخصوصية [الرابط].

Use: Checkout page, below the order button. Do not tick any box for the customer.

B. Checkout: optional marketing email opt-in (unticked checkbox)

☐ Yes, [Company legal name] may send me offers and updates about its products and services by email. I can withdraw this consent at any time using the unsubscribe link or by contacting [email].

☐ نعم، أوافق على أن ترسل [الاسم القانوني للشركة] إليّ عروضاً وتحديثات عن منتجاتها وخدماتها عبر البريد الإلكتروني. يمكنني سحب موافقتي في أي وقت من خلال رابط إلغاء الاشتراك أو بالتواصل عبر [البريد الإلكتروني].

Use: Checkout and account sign-up. Checkbox must start unticked and be separate from terms.

C. Contact or enquiry form notice

We will use your name and email only to reply to your enquiry. Details are in our Privacy Notice [link].

سنستخدم اسمك وبريدك الإلكتروني للرد على استفسارك فقط. التفاصيل في إشعار الخصوصية [الرابط].

Use: Under the submit button of every web form.

D. Newsletter sign-up and email footer

Sign up: ☐ I want to receive the [Company] newsletter. Footer: You receive this email because you subscribed at [source] on [date]. Unsubscribe | Preferences | Privacy Notice

للاشتراك: ☐ أرغب في تلقي النشرة الإخبارية لـ [الشركة]. تذييل الرسالة: تصلك هذه الرسالة لأنك اشتركت عبر [المصدر] بتاريخ [التاريخ]. إلغاء الاشتراك | التفضيلات | إشعار الخصوصية

Use: Sign-up form and every marketing email.

10. Bilingual Consent Copy Blocks (2): WhatsApp and Cookies

Keep proof of every opt-in: who, when, which text, which channel. Make withdrawal as easy as giving consent.

E. WhatsApp marketing opt-in (web form or checkout, unticked)

☐ I agree to receive marketing messages from [Company] on WhatsApp at [number]. I can reply STOP at any time to unsubscribe.

☐ أوافق على تلقي رسائل تسويقية من [الشركة] عبر واتساب على الرقم [الرقم]. يمكنني إلغاء الاشتراك في أي وقت بإرسال كلمة «إيقاف».

Use: Never message a number you did not collect consent for. Do not buy or scrape contact lists.

F. WhatsApp welcome and opt-out confirmation messages

Welcome: You are subscribed to [Company] updates on WhatsApp. Reply STOP to unsubscribe at any time. | Opt-out: You have been unsubscribed and will receive no further marketing messages. Reply START to subscribe again.

الترحيب تم اشتراكك في تحديثات [الشركة] على واتساب. أرسل «إيقاف» لإلغاء الاشتراك في أي وقت. | الإلغاء تم إلغاء اشتراكك ولن تصلك رسائل تسويقية أخرى. أرسل «ابدأ» للاشتراك مرة أخرى.

Use: Send the welcome message straight after opt-in. Process STOP replies the same day.

G. Cookie banner

We use essential cookies to run this site. With your permission we also use analytics and marketing cookies. [Accept all] [Reject non-essential] [Choose]

نستخدم ملفات تعريف الارتباط الأساسية لتشغيل هذا الموقع. وبموافقتك نستخدم أيضاً ملفات تحليلية وتسويقية. [قبول الكل] [رفض غير الأساسية] [تخصيص]

Use: Analytics and marketing scripts must not load until the visitor chooses. Reject must be as prominent as Accept.

H. Consent withdrawal confirmation

Your consent was withdrawn on [date]. We will stop using your data for [purpose]. You can opt in again at any time at [link].

تم سحب موافقتك بتاريخ [التاريخ]. سنتوقف عن استخدام بياناتك لأغراض [الغرض]. يمكنك الاشتراك من جديد في أي وقت عبر [الرابط].

Use: Send within the same day the request is received.

Consent rules behind these blocks: affirmative action, specific purpose, separate from other terms, informed, as easy to withdraw as to give, and recorded. Have your Arabic wording reviewed by a qualified specialist before publishing.

11. Your 30-Day Action Plan and Self-Check

Small steps, in order. Assign a name and a date to every line.

Week	Focus	Actions
1	Scope and owner	• Name a privacy owner and a breach incident lead and deputy • Complete the applicability check (page 3) • List every system, tool and vendor that touches personal data
2	Records	• Interview each department and build the RoPA (pages 4 and 5) • Reconcile the RoPA with the vendor list • Record every transfer outside the UAE
3	Vendors and breach	• Review Tier 1 vendors and sign or save their DPAs (pages 6 to 8) • Agree the breach workflow and write down contact numbers (pages 9 and 10)
4	Consent and training	• Replace consent wording and cookie banner (pages 11 and 12) • Brief every team that handles customer or staff data for 30 minutes • Diary the next RoPA and vendor review dates

15-point readiness self-check

#	Statement	Yes
1	We know whether the PDPL applies to each of our entities	☐
2	We know where we act as controller and where as processor	☐
3	A RoPA exists and every department is covered	☐
4	Every RoPA row has a lawful ground and a retention rule	☐
5	Every vendor appears in the RoPA and has an owner	☐
6	Tier 1 vendors have a signed DPA or accepted standard terms	☐
7	We have recorded every transfer outside the UAE and its mechanism	☐
8	Our privacy notice is current, dated, and available in Arabic and English	☐
9	Marketing consent is separate, unticked, recorded and withdrawable	☐
10	Analytics and marketing cookies stay off until the visitor chooses	☐
11	We have a named person and process to handle rights requests	☐
12	We have a breach lead, deputy, contact list and written workflow	☐
13	Staff who handle personal data have had privacy training	☐
14	Access to systems uses unique accounts and multi-factor authentication	☐
15	We review the RoPA and vendor list at least once a year	☐

How to read your score: 13 to 15 ticks: maintain and review. 8 to 12: close the gaps in the 30-day plan. Under 8: start with pages 3, 4 and 9, and consider an independent diagnostic.

12. Glossary, Where to Verify, and Next Steps

Term	Meaning
Controller	The person that decides why and how personal data is processed
Processor	The person that processes personal data on behalf of a controller
Data subject	The individual the personal data is about
RoPA	Records of processing activities (the register kept under Articles 7 and 8)
DPA	Data processing agreement between a controller and a processor, or a processor and a sub-processor
DPIA	Data protection impact assessment for high-risk processing (Article 21, working reference)
DPO	Data protection officer (Articles 10 to 12, working reference)
Data Office	The UAE Data Office, the authority created by Federal Decree-Law No. 44 of 2021

Where to verify before you rely on anything here

- The official text of Federal Decree-Law No. 45 of 2021 on the UAE Legislation portal and in the Official Gazette.
- Official announcements and publications of the UAE Data Office, including any Executive Regulations or guidance.
- Your sector regulator, if you hold health, banking or credit data.
- DIFC or ADGM authorities if you are licensed there.

About FyrahPrivacy

FyrahPrivacy is a UAE data privacy architecture and compliance engineering consultancy. We build the registers, workflows, bilingual notices and controls that make UAE PDPL compliance operational and evidenced, with fixed scope and fixed fees.

Service	What you get
UAE PDPL Audit Dossier	7 business days: scorecard, RAG matrix and remediation plan; the fee is credited toward a Sprint within 30 days
Rapid Baseline and Enterprise Shield Sprints	14 and 30 calendar days: RoPA, bilingual notices, cookie governance, rights and breach workflows, transfers, DPIA
Vendor Risk & DPA Pack	5 business days: bilingual master DPA, sub-processor register, questionnaire, negotiation sheet
Staff Privacy Training and Fractional DPO	3 business days of training; ongoing DPO retainer with defined response times

BOOK A FREE 20-MINUTE OPERATIONAL REVIEW

Website: fyrahprivacy.com **Email:** contact@fyrahprivacy.com

Phone: +971 50 807 2890 **Location:** Dubai, UAE

Statutory Notice: FyrahPrivacy is a specialized data privacy engineering and compliance consultancy practice, not a licensed UAE law firm. We deliver operational compliance artifacts, technical configurations, and data governance frameworks. Our deliverables do not constitute formal legal representation before judicial courts. This blueprint is general guidance, not legal advice.