Z&Co.
الزمخشري ومشاركوه



INSIGHT 28 October 2026 · 18 min read

CLOUD COMPUTING SPECIAL ECONOMIC ZONE

Saudi Arabia's cloud computing zone: two decisions for technology and data groups run from abroad



Martin Creek
Partner, Corporate, Commercial & Finance Transactions



Sarah Sadek
Counsel, Regulatory & Advisory

16 September 2026
ZONE REGULATION IN FORCE

5 November 2026
SDAIA CONSULTATION CLOSES

8 December 2026
LICENSING GUIDE DUE

Contents

	At a glance	3
01	Two decisions, and why now	4
02	Where data centres can sit, and where the business must be run	6
03	Hosting: where Saudi data must sit today	7
04	Tax: what the zone offers, and what it does not	10
05	Economic substance: running the business from the zone	12
06	Licensing: conditions and timing	14
07	Data protection: obligations that apply regardless of the zone	15
08	What to do now	18
09	In short	19
	The regulators in this article	20

WHO THIS IS FOR

For general counsel and finance leaders of technology and data groups (cloud and data-centre operators, software and platform businesses, fintechs) that manage their Saudi business from outside the Kingdom.

At a glance

IN SHORT

The zone's rules are in force, and its core conditions are knowable now, before CST issues its licensing guide. For a group run from abroad, the zone's value lies in tax certainty rather than a lower rate, and it comes with the obligation to run the licensed entity from the zone. The nearer deadline is the data one. If SDAIA's draft amendments to the data protection rules are adopted as published, where your Saudi personal data is stored may no longer be entirely your choice, and the consultation closes on 5 November.

WHAT TO DO NOW

1. **Decide where personal data from the Kingdom will sit.**
2. **Assess the tax case at the standard rate.**
3. **Map the IP early.**
4. **Decide who the Saudi customers will be.**
5. **Model the commitments, not just the incentives.**
6. **Check the activity qualifies when the licensing guide is issued.**

THE REGULATORS IN THIS ARTICLE

ECZA
Economic Cities and Special Zones Authority

CST
Communications, Space and Technology Commission

NCA
National Cybersecurity Authority

ZATCA
Zakat, Tax and Customs Authority

SDAIA
Saudi Data and Artificial Intelligence Authority

SAMA
Saudi Central Bank

01 Two decisions, and why now

If your group holds its Saudi personal data only abroad, you may need to store it in the Kingdom if the proposed data protection amendments are adopted. If the Cloud Computing Special Economic Zone (the zone) is on your list for the 5% corporate income tax rate, this zone does not offer it.

Two developments lie behind that. The first is that the zone's rules are in force: its zone regulation took effect on publication in the Official Gazette on 16 September 2026, joining the organisational regulation, which has applied since April 2026. The Communications, Space and Technology Commission (CST) must issue the licensing guide by 8 December 2026, 90 days after the zone regulation was approved on 9 September; the guide will set the licensing procedure and the list of qualifying activities. Unlike the Kingdom's other three special economic zones, which offer a 5% rate for 20 years on qualifying activities, the cloud zone's tax incentives are a set of OECD-based treatments. As in the other zones, a licensed entity must be run from the zone. Failure to do so is treated as a licensing violation and puts the entity's incentives at risk.

The second is that the Saudi Data and Artificial Intelligence Authority (SDAIA) is consulting, until 5 November 2026, on draft amendments to the implementing regulation of the Personal Data Protection Law. Today the law sets conditions for sending personal data abroad but imposes no general requirement to store it in the Kingdom, and the cloud and essential controls of the National Cybersecurity Authority (NCA) have not required in-Kingdom hosting since 2024. As published for consultation, the draft would add a storage requirement, while still allowing transfers abroad under the transfer rules. If it is adopted as published, and your Saudi personal data sits only on infrastructure abroad, you may need to store it in the Kingdom.

That makes two decisions pressing for you: where your Saudi data will be stored, and whether, and on what terms, to set up a licensed entity in the zone.

Both are better settled now than after building. Hosting set up abroad today may have to be brought into the Kingdom if SDAIA adopts its draft, and a Saudi entity is costly to restructure once in place. This article starts with the zone itself (where data centres can sit and which activities qualify), then turns to the hosting rules that apply whatever the zone says, the tax and substance rules, licensing, and data protection. It ends with six decisions to take now.

EXHIBIT 1

Key dates

December 2025	**NCA private-sector controls**	Controls for notified private-sector entities outside critical national infrastructure
April 2026	**Organisational regulation applies**	The zone's organisational regulation
7 August 2026	**Economic substance regulation applies**	In all four special economic zones
August 2026	**ZATCA procedural guide issued**	Describes the zone and its qualifying activities
9 September 2026	**Zone regulation approved**	By the ECZA board
16 September 2026	**Zone regulation in force**	On publication in the Official Gazette
5 November 2026	**SDAIA consultation closes**	Draft amendments to the Personal Data Protection Law's implementing regulation
8 December 2026	**CST licensing guide due**	Licensing procedure and list of qualifying activities

02 Where data centres can sit, and where the business must be run

The procedural guide of the Zakat, Tax and Customs Authority (ZATCA) describes the zone as located in Riyadh but not tied to a specific site, and says licensed entities may set up and operate data centres throughout the Kingdom.

The zone's regulations do not say this. The organisational regulation governs the zone's activities in line with its approved location and maps, and the zone regulation says a licence covers activity inside the zone; activity outside it must follow the procedures that apply in the rest of the Kingdom.

ZATCA's guide does not amend the regulations, so confirm with CST, for each data-centre site you plan, that your licence will cover it.

Where the business is run from is fixed. A company set up in the zone must have its head office there. Whether your licensed entity is a zone company or a branch of a foreign company, the economic substance rules (below) require its qualifying activities to be directed and managed from within the zone.

Which activities attract the incentives

Only qualifying activities attract the zone's incentives. ZATCA's procedural guide, issued in August 2026, describes them as activities related to cloud computing and informatics services, including information technology and programming, financial technology, Industry 4.0, digital health and smart mobility, and any others set by decision. The zone regulation, published more recently, defines them as activities within the zone's targeted sectors and leaves the list of qualifying main and sub-activities to CST's licensing guide. You will therefore need to confirm with CST that your activity qualifies once the licensing guide is out.

Supporting activities, meaning activities not designated as qualifying, need a licence under mainland procedures and CST's approval to operate in the zone, and do not attract the zone's incentives.

03 Hosting: where Saudi data must sit today

The zone's rules must be read alongside the hosting requirements that apply to particular data and customers.

The NCA's cloud and essential controls no longer require data or cloud services to be hosted in the Kingdom. The NCA removed those requirements in 2024 and moved data localisation to SDAIA. Organisations subject to those controls must now consult SDAIA's National Data Management Office before taking any action on data localisation. Beyond that, where data must sit depends on whose data it is and who the customer is, in addition to the personal-data transfer rules below:

Government data

Government entities must host their websites, email, information and services, and the systems these need, in the Kingdom. They may do so themselves, through another government body, or through a hosting provider licensed by the communications regulator, now CST. CST's cloud computing regulations go further: government data must be placed with a CST-registered provider and may not leave the Kingdom for any purpose, even temporarily for caching or backup, unless another law expressly allows it.

Banks and other financial institutions

The Cyber Security Framework of the Saudi Central Bank (SAMA) is mandatory for the banks, financing companies and other institutions SAMA regulates. For public and hybrid cloud, it says they should in principle use only services located in Saudi Arabia, and should obtain SAMA's explicit approval to use a service abroad. They should also obtain SAMA's approval before using any public or hybrid cloud service or signing the contract.

Critical systems

These are systems that a government body or other organisation identifies as critical under the NCA's criteria. Remote access to them from outside the Kingdom is barred. They, and any part of their technical components, may be hosted only in-house or in cloud services provided by government bodies or by national companies that comply with the NCA's cloud controls. Outsourced and managed services on these systems must also come from national companies or entities.

The critical-systems rule applies alongside the government-hosting rules, not instead of them. A provider wanting to host a government entity's critical systems must therefore meet both: it must be licensed by CST (and, for cloud services, registered with it), and it must be a national company that complies with the NCA's cloud controls.

Whether a foreign-owned group can meet the second test by incorporating in the zone is not settled. The binding Arabic of the critical-systems controls says "national companies", where the English translation says "Saudi companies", and those controls do not define the term, so it could be read as requiring Saudi ownership rather than Saudi incorporation. A licensee would point to the zone's organisational regulation, which deems a company established under it to be of Saudi nationality. That provision, however, sits in the rules on companies formed in the zone and does not refer to the NCA's controls. A licensed branch of a foreign company cannot rely on it at all, because a branch is not a company formed in the zone.

Rules for cloud service providers

The Cloud Cybersecurity Controls apply to a provider because of its customers, not its place of incorporation. A provider serving a Saudi government body or critical national infrastructure is within their scope; a provider serving neither is outside them, although the separate private-sector controls described below may still apply. Separately from the NCA's controls, CST's cloud computing regulations require a provider to register with CST before it takes direct or effective control of a data centre, or of key cloud infrastructure, in the Kingdom that is used to provide cloud services.

Two obligations deserve particular attention. First, cybersecurity roles at a provider's data centres in the Kingdom must be filled by qualified Saudi nationals: mandatory for the three higher data classification levels, optional for the lowest. Second, the cloud controls require in-scope providers to implement the NCA's Essential Cybersecurity Controls as well. Those add two rules of their own: all cybersecurity positions, not only those at data centres, must be filled by full-time, competent Saudi nationals; and outsourced security monitoring that uses remote access must be run from inside the Kingdom.

The 2025 private-sector controls

Since December 2025 the NCA has also had a further set of controls for notified private-sector entities outside critical national infrastructure. Large notified entities, those with more than 250 full-time staff or more than SAR 200 million in annual revenue, must fill the post of head of their cybersecurity function, and the supervisory and sensitive roles within it, with full-time, highly competent Saudi nationals. That applies whoever their customers are. For smaller notified entities, this is recommended rather than required.

EXHIBIT 2

Where cybersecurity roles must, or should, be filled by Saudi nationals

MANDATORY AT THE THREE HIGHER LEVELS	MANDATORY	MANDATORY	RECOMMENDED
Cloud providers within the Cloud Cybersecurity Controls Cybersecurity roles at data centres in the Kingdom For the three higher data classification levels; optional for the lowest	**The same providers, through the Essential Cybersecurity Controls** All cybersecurity positions, full-time	**Large notified private-sector entities** Head of cybersecurity, and the supervisory and sensitive roles within the function More than 250 full-time staff or more than SAR 200 million in annual revenue	**Smaller notified private-sector entities** The same roles
Applies because of the provider's customers		Applies whoever the customers are	

Note: The Essential Cybersecurity Controls also require outsourced security monitoring that uses remote access to be run from inside the Kingdom.



04 Tax: what the zone offers, and what it does not

Licensed entities in the cloud zone pay corporate income tax at the standard rate of 20%, the same as on the mainland.

Saudi-source payments to non-residents that fall within the withholding tax rules bear tax at the ordinary rates of 5% to 20%, depending on the type of payment and any applicable treaty, subject to the classification rule below. For VAT and customs, the zone is treated as mainland.

What the zone offers instead is a set of tax treatments anchored in international agreements and OECD principles. ZATCA's guide applies them subject to the global minimum tax rules, for companies within those rules' scope. The most distinctive is that a non-resident's use or storage of data in data centres in the Kingdom does not, of itself, create a virtual permanent establishment. ZATCA notes in its guide that it does not apply that concept in any event, so the rule gives certainty rather than new relief. The live question is whether a server or other fixed place amounts to a permanent establishment, and that remains fact-specific under the OECD commentaries.

The other treatments are the classification of payments to related parties connected with zone activities according to OECD principles, discussed below, and the application of the OECD commentaries to payments to residents of treaty countries, particularly on permanent establishments, including how profits are attributed to them. The zone also provides for mutual agreement procedures to resolve tax disputes where a tax treaty applies, and for the deduction of payments to related parties, provided they comply with the transfer pricing rules.

The classification rule may be worth more than it looks. ZATCA's guide says that related-party payments classified on OECD principles may not be subject to Saudi withholding tax at all, and may be taxed only in the recipient's country, typically where a tax treaty gives that country the sole right to tax them. The guide's own example is a fee for software that the payer may copy for use in its own business: a royalty under ZATCA's mainland practice, but business profits under the OECD commentaries, which is the treatment the cloud zone will apply. How far this reaches is left to the zone's guide on exemptions and incentives, to be issued by the Economic Cities and Special Zones Authority (ECZA), which oversees the zones; it had not been published when this article was written.

If your main concern is that infrastructure in the Kingdom could give your group companies abroad a taxable presence there, these treatments may be worth more to you than a reduced

tax rate, depending on your circumstances and the applicable tax treaties. The economic substance rules below also apply: a licensed entity that fails them faces penalties, and CST treats the failure as a licensing violation.

By comparison, for qualifying activities, King Abdullah Economic City, Jazan and Ras Al Khair offer 5% corporate income tax for 20 years and, on ZATCA's reading, an exemption from withholding tax on payments to non-residents, subject to anti-avoidance and reporting requirements. Saudi- and GCC-owned licensed entities also pay the 5% rate, instead of zakat. ZATCA's guide says these incentives will be reviewed for companies within the global minimum tax rules once the Kingdom applies those rules. The three zones also offer VAT and customs relief on goods brought in for qualifying activities, which the cloud zone does not.

EXHIBIT 3

Tax and levy treatment: the cloud zone and the other three special economic zones

FOR LICENSED ENTITIES	CLOUD COMPUTING ZONE	KING ABDULLAH ECONOMIC CITY, JAZAN, RAS AL KHAIR
Corporate income tax	20%, the standard rate, as on the mainland	5% for 20 years on qualifying activities
Withholding tax on payments to non-residents	Ordinary rates of 5% to 20%, subject to the OECD-based classification rule	Exempt for qualifying activities, on ZATCA's reading; subject to anti-avoidance and reporting requirements
VAT and customs	Treated as mainland	Relief on goods brought in for qualifying activities
Zakat	Zakat Collection Law does not apply; 20% income tax instead	Zakat Collection Law does not apply; Saudi- and GCC-owned entities pay the 5% rate on qualifying activities
Expatriate levy	Exempt for workers and their dependants in their zone (all four zones)	
OECD-based treatments	No virtual permanent establishment from data use or storage alone; OECD classification of related-party payments; OECD commentaries for treaty residents; mutual agreement procedures where a tax treaty applies; deduction of related-party payments that comply with transfer pricing rules	Not among these zones' listed incentives

Note: For companies within the global minimum tax rules, ZATCA's guide applies the cloud zone's treatments subject to those rules, and says the other three zones' incentives will be reviewed once the Kingdom applies those rules.

Two further points apply in all four zones. First, the Zakat Collection Law does not apply to licensed entities; they pay income tax instead. In the cloud zone that means 20% income tax in place of zakat, so if your group is Saudi- or GCC-owned and pays zakat on its Saudi business today, model the switch before counting the zone as a saving. Second, licensed entities are exempt from the expatriate levy for their workers and their dependants in their zone.

05 Economic substance: running the business from the zone

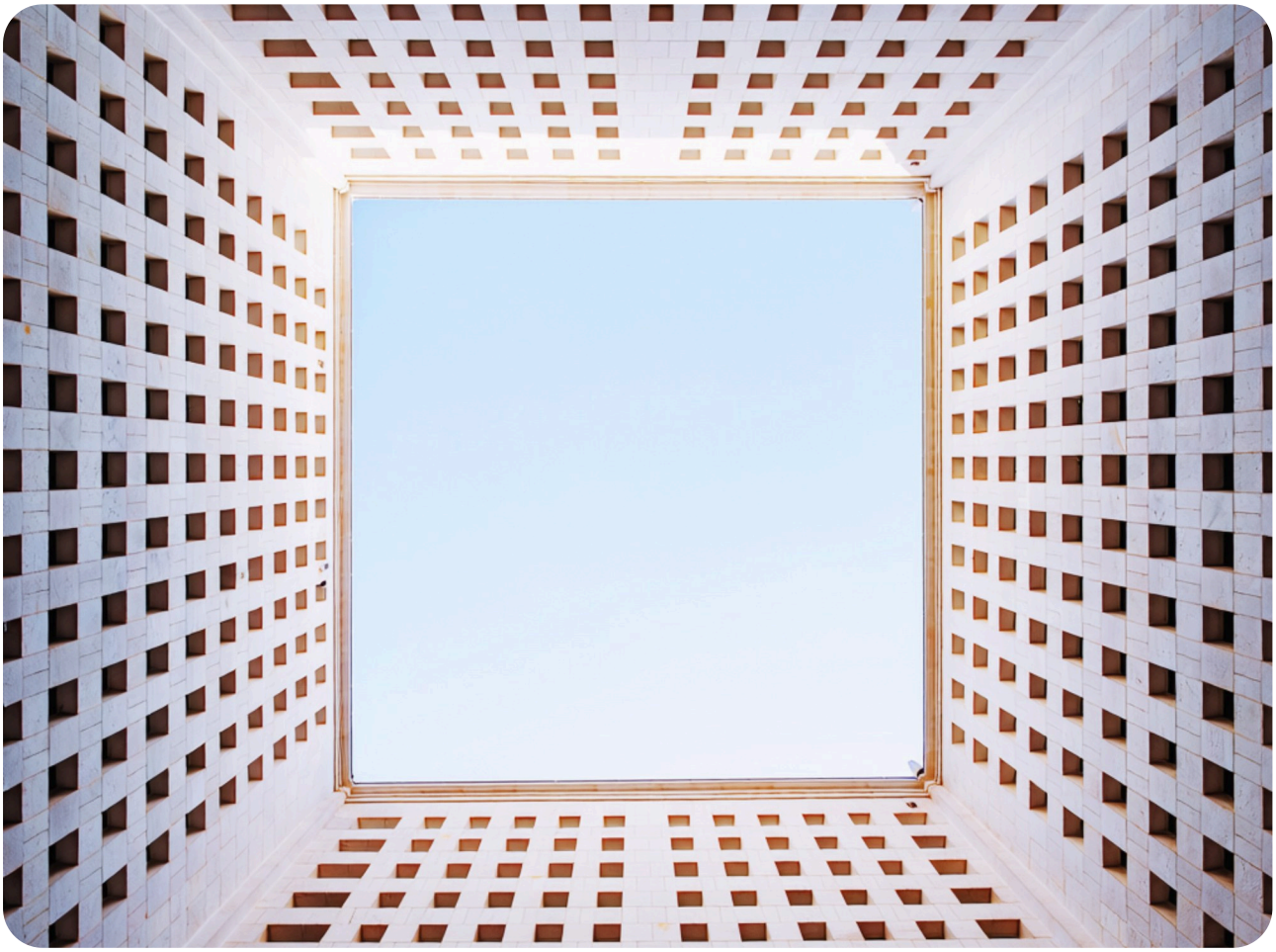
ZATCA's economic substance regulation has applied in all four zones since 7 August 2026.

A licensed entity directed from headquarters abroad puts its incentives at risk: breaches attract penalties issued by ECZA, and in the cloud zone CST treats them as licensing violations. Each year, starting with its first financial year of qualifying activities, a licensed entity must:

- Have suitable premises and assets in the zone for its qualifying activities;
- Have enough full-time staff physically present in the zone for those activities (staff employed by its contractors count);
- Incur operating expenditure in the zone in proportion to those activities;
- Have those activities directed and managed from within the zone by suitably qualified managers, at least one of whom is resident in the Kingdom;
- Hold board meetings that take and minute real strategic decisions, with their quorum reached in the Kingdom; and
- File an annual return with ZATCA.

Additional tests apply where a licensed entity's qualifying activities involve intellectual property (IP). If you are weighing the zone as a place to hold platform IP, this is the provision to read first. IP activities count as qualifying activities only as ECZA classifies them, and an entity carrying them on must also:

- Have at least half the managers running its qualifying activities resident in the Kingdom;
- Have a detailed business plan that justifies holding the IP in the zone;
- Provide detailed information about its staff, including their experience, qualifications, contracts and length of service;
- Take its strategic decisions for the IP, and manage and bear its risks, inside the zone; and
- Not limit its activity to marketing IP assets. Income from IP activities related to marketing those assets gets no incentives at all.



06 Licensing: conditions and timing

Two quantitative conditions apply throughout the licence, and CST checks them: capital expenditure of at least SAR 1 million in the first five years, and investment in R&D of at least 1.5% of fixed assets.

SAR 1M
Minimum capital expenditure in the first five years

1.5%
Minimum R&D investment, as a share of fixed assets

SAR 15M
Example: R&D floor on SAR 1 billion of data-centre assets

For an asset-heavy investor, the second is the demanding one: on SAR 1 billion of data-centre assets, the R&D floor is SAR 15 million. Unlike the capital-expenditure requirement, the R&D requirement has no specified measurement period: the zone regulation does not say whether the 1.5% is measured annually or cumulatively, nor what counts as R&D investment. The licensing guide, which must include the forms for assessing these criteria, should answer both questions. Until it does, model both readings.

Only CST may license qualifying activities in the zone. It does so in coordination with the Royal Commission for Riyadh City, and reports its licences to ECZA, which oversees the zones. Applicants must submit a statement proving their technical competence and financial capacity, and a business plan. CST also assesses each project against qualitative criteria: limiting relocation from other regions of the Kingdom and the risk of unfair competition with them, developing highly skilled talent, contributing to product complexity, and the investor's credibility and commitment. Priority goes to investors who will deepen value chains in other regions of the Kingdom.

On timing, CST must issue its licensing guide within 90 days of the regulation being issued, which is by 8 December 2026, counting from the ECZA board's approval on 9 September. The guide will set out the licensing procedure, the qualifying activities and the forms used to assess applicants. CST's fee schedule follows separately: it is added to the guide once ECZA's board approves it, and the regulation makes clear that the 90-day deadline does not wait for it. The December guide may therefore tell applicants what they must do, but not yet what CST will charge. The core conditions are already in the regulation, and you can prepare against them now.

07 Data protection: obligations that apply regardless of the zone

The zone texts contain no data protection rules of their own, so the Personal Data Protection Law applies in the zone as it does elsewhere in the Kingdom.

It also covers processing outside the Kingdom of personal data about people residing in it. Your hub abroad is therefore already within its reach. Personal data may be transferred or disclosed abroad only for a purpose the law permits, and only if doing so does not harm national security or the Kingdom's vital interests. Transfers are also subject to two conditions: they must be limited to the minimum personal data needed, and the destination must provide at least the level of protection Saudi law requires, as assessed by SDAIA. The transfer rules can exempt the controller from either or both conditions, including through the intra-group route described below.

SDAIA must publish a list of the countries and international organisations that meet that standard, and review it every four years or sooner where needed. The same assessment applies to cities, special economic zones and global trade centres. A hub in a UAE free zone is therefore not adequate by default, but it can be assessed, and listed, in its own right.

For personal data from the Kingdom that runs through your hub abroad, the intra-group route is the one to build on. It can lift the adequacy condition, the minimum-necessary condition or both, but only on terms. The transfer must be necessary for centralised operations of a multinational group. The controller and its affiliates must commit to binding common rules or standard contractual clauses, unless the recipient is certified by a body SDAIA has licensed. A transfer risk assessment is required before the data moves, as it is for any continuous or large-scale transfer of sensitive data. If the safeguards are not applied, or SDAIA finds them inadequate, the exemption falls away and the transfers must stop.

SDAIA is consulting until 5 November 2026 on amendments to the law's implementing regulation. As published for consultation, the draft would require controllers to store personal data in the Kingdom, while still allowing transfers abroad under the transfer rules. Read literally, the storage duty applies even where data is also transferred abroad. Another reading is that in-Kingdom storage is only the default, and a lawful transfer is enough on its own. The draft would also make transferring or disclosing personal data abroad one of the triggers for registering in SDAIA's national register of controllers. If adopted as drafted, the amendments would take effect 60 days after publication in the Official Gazette.

EXHIBIT 4

How personal data can leave the Kingdom

01

Permitted purpose

Only for a purpose the law permits, and only if it does not harm national security or the Kingdom's vital interests

02

Two conditions

- Limited to the minimum personal data needed
- Destination gives at least the protection Saudi law requires, as assessed by SDAIA

How adequacy is assessed

SDAIA lists adequate countries and international organisations, and can assess cities, special economic zones and global trade centres

INTRA-GROUP ROUTE · CAN LIFT EITHER OR BOTH CONDITIONS

- ✓ Necessary for centralised operations of a multinational group
- ✓ Binding common rules or standard contractual clauses, unless the recipient is certified by a body SDAIA has licensed
- ✓ Transfer risk assessment before the data moves

If the safeguards are not applied, or SDAIA finds them inadequate, the exemption falls away and the transfers must stop.

DRAFT · CONSULTATION TO 5 NOVEMBER 2026

Controllers would have to store personal data in the Kingdom, with transfers still allowed under the transfer rules. Transfers abroad would trigger registration. In effect 60 days after publication, if adopted as drafted.

Beyond transfers, two obligations are easy to miss when your data function sits outside the Kingdom. The first is impact assessments, which the implementing regulation requires in four cases:

- Processing sensitive data;
- Combining, comparing or linking datasets from different sources;
- Processing that, on a large scale or repeatedly, involves people who lack full legal capacity, continuous monitoring, emerging technologies or automated decisions; and
- Offering a product or service whose processing is likely to cause serious harm to privacy.

For a cloud or platform business, those triggers describe ordinary design decisions, often taken by your teams outside the Kingdom, so a platform migration will often be an

assessment event rather than an edge case. Two phrases in the third case read differently in SDAIA's own English translation: the gazetted Arabic says "large-scale or repeated", where the English says "large scale and repetitive", and "emerging technologies", where the English says "newly adopted technologies". Both differences affect when the duty arises, and the Arabic governs.

The second is the breach clock. A personal data breach must be notified to SDAIA within 72 hours of the controller becoming aware of it, where it could harm the data or the individual, or conflict with their rights or interests. Affected individuals must be told without undue delay where it could damage their data or conflict with their rights or interests. Where detection sits with your security function abroad, settle now how a breach found there reaches the controller, and at what point SDAIA could treat the controller as aware. That point is when the 72-hour clock starts.

72 hrs
From becoming aware, to notify SDAIA of a breach that could cause harm

5 yrs
Records of processing kept after processing ends

60 days
From Official Gazette publication to effect, if adopted as drafted

4 yrs
Maximum interval for SDAIA to review its adequacy list

Two standing duties complete the picture. Records of processing must be kept for as long as the processing continues and for five years after it ends. A data protection officer must be appointed where a controller's core activities consist of processing that requires regular and systematic monitoring of individuals, or of processing sensitive personal data. A platform built on tracking its users should expect to meet that test.

Security is where data protection meets the cybersecurity rules discussed above. The implementing regulation requires controllers bound by the NCA's controls to comply with them, and others to follow recognised cybersecurity practices and standards.

08 What to do now

1

Decide where personal data from the Kingdom will sit.

Government bodies, banks and critical-system operators already carry their own location rules. Other personal data may sit abroad today if the transfer rules above are met. SDAIA's draft, as published, would add a requirement to store personal data in the Kingdom. Anyone with a view on the draft can respond on the Istitlaa platform until 5 November 2026.

2

Assess the tax case at the standard rate.

The cloud zone has no reduced rate and no general withholding tax exemption. Ask whether the virtual permanent establishment rule and the other OECD-based treatments address a real risk in your structure. If they do, the zone may be attractive. If the attraction was the rate, it is not there.

3

Map the IP early.

If your plan involves holding or exploiting platform IP in the zone, the additional substance tests for IP apply, and income from marketing IP gets no incentives at all.

4

Decide who the Saudi customers will be.

Serving government bodies, or private entities that own, operate or host critical national infrastructure, brings a provider within the Cloud Cybersecurity Controls. That market is open rather than closed: government entities may host through a licensed provider, not only in-house. If that is your plan, start hiring now. In-scope providers must fill cybersecurity roles at their data centres in the Kingdom with qualified Saudi nationals, and because the cloud controls also require the Essential Cybersecurity Controls, that rule extends to all cybersecurity positions, not just data-centre roles. Scope the hiring before budgeting it. The hiring question may not wait on the customer question at all: under the private-sector controls, a large entity the NCA notifies must have Saudi nationals heading cybersecurity and in its supervisory and sensitive roles, whoever its customers are.

5

Model the commitments, not just the incentives.

The R&D commitment, at least 1.5% of fixed assets throughout the licence, scales with the size of the build. The zone regulation does not say how it is measured, so model both an annual and a cumulative reading until CST's licensing guide, which must include the forms for assessing it, shows which applies.

6

Check the activity qualifies when the licensing guide is issued.

The incentives attach to qualifying activities only; supporting activities carried on in the zone are expressly excluded. CST must issue its licensing guide, with the list of qualifying activities, by 8 December 2026. An activity near the edge of ZATCA's description is a question to confirm with CST then, not to assume now.

09 In short

The zone is open, and its core conditions are knowable now, before the guide. For a group run from abroad, the zone's value lies in tax certainty rather than a lower rate, and it comes with the obligation to run the licensed entity from the zone. The nearer deadline is the data one. If SDAIA's draft is adopted as published, where your Saudi personal data is stored may no longer be entirely your choice, and the consultation closes on 5 November.

If your group runs its Saudi technology or data business from outside the Kingdom and would like a short check of its zone, tax, hosting and data assumptions against the gazetted texts before the licensing guide is issued, Martin Creek and Sarah Sadek would be glad to talk.

AUTHORS

For further advice and information



Martin Creek
Partner, Corporate, Commercial & Finance Transactions

Martin.Creek@zamakhchary.com



Sarah Sadek
Counsel, Regulatory & Advisory

Sarah.Sadek@zamakhchary.com

For other questions about this article or the firm, contact us at **info@zamakhchary.com**.

The regulators in this article

Six authorities set the rules described in this article:

ABBREVIATION	AUTHORITY	ROLE IN THIS ARTICLE
ECZA	**Economic Cities and Special Zones Authority**	Its board approved the zone regulation, and it will issue the zone's guide on exemptions and incentives.
CST	**Communications, Space and Technology Commission**	It licenses qualifying activities in the zone, in coordination with the Royal Commission for Riyadh City, and will issue the licensing guide. Under its cloud computing regulations it also registers providers that control data centres or key cloud infrastructure in the Kingdom.
NCA	**National Cybersecurity Authority**	It issues the cybersecurity rulebooks. The Cloud Cybersecurity Controls apply to government and critical national infrastructure entities that use cloud services and to the providers that serve them, and in-scope providers must also implement the Essential Cybersecurity Controls. Separate controls cover critical systems and, since December 2025, notified private-sector entities.
ZATCA	**Zakat, Tax and Customs Authority**	It administers tax and customs, and has issued a procedural guide for the zones and the economic substance regulation.
SDAIA	**Saudi Data and Artificial Intelligence Authority**	It enforces the Personal Data Protection Law, and its National Data Management Office is now the reference point for data localisation.
SAMA	**Saudi Central Bank**	It sets location and approval rules for cloud use by the banks and other institutions it regulates.

Z & Co.

الزمخشري ومشاركوه

Zamakhchary.com · info@zamakhchary.com

The content of this article is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances.

© 2026 Zamakhchary & Co. All rights reserved.