Cloud Compliance Center - Malaysia

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

Malaysia

*This content was last reviewed around April 2023.*

**Cloud-neutral**

**1. Are financial institutions legally permitted to use cloud services?**

Yes, subject to compliance with the applicable guidelines, rules, directives and guidance issued by the Securities Commission Malaysia and Bank Negara Malaysia.

**2. Are there any rules that apply to cloud use by financial institutions (e.g., rules regarding outsourcing or the use of cloud services)?**

Yes. The Risk Management in Technology Guidelines issued by Bank Negara Malaysia ("**BNM**") provide the following:

A financial institution must conduct a comprehensive risk assessment prior to cloud adoption. The risk assessment must consider the inherent architecture of cloud services that leverages on the sharing of resources and services across multiple tenants over the internet. The risk assessment must be documented and made available for BNM's review as and when requested.

A financial institution must notify BNM of its intention to use cloud services for noncritical systems.

A financial institution is required to consult BNM prior to using public cloud for critical systems.

A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorized disclosure and access.

Where the use of cloud services constitutes outsourcing, the financial institution must conduct appropriate due diligence of a service provider when considering all new arrangements, and when renewing or renegotiating existing arrangements.

Further, where the financial institution is a holder of a capital markets and services license ("**CMSL Holder**"), the Licensing Handbook issued by the Securities Commission Malaysia provides that a CMSL Holder is not allowed to outsource any back office function that involves (i) the financial institution's decision-making functions or (ii) any interaction or direct contact with the financial institution's clients. Therefore, where the provision of cloud outsourcing services does not involve (i) or (ii), it will be permissible for the financial institution to outsource using those cloud services.

**3. Are there any specific contractual requirements for cloud outsourcing?**

Under the Risk Management in Technology Guidelines, a financial institution must establish service level agreements when engaging third-party service providers (e.g., cloud services providers). These must be regularly reviewed to take into account the latest security and technological developments in relation to the services provided. The service level agreement should contain the following:

Access rights for the regulator and any party appointed by the financial institution to examine any activity or entity of the financial institution

Requirements for the service provider to provide sufficient prior notice to financial institutions of any subcontracting that is substantial

A written undertaking by the service provider on compliance with secrecy provisions under relevant legislation

Arrangements for disaster recovery and backup capability, where applicable

Critical system availability

Arrangements to secure business continuity in the event the service provider exits or is terminated

Other terms that are to be included in an outsourcing arrangement arising through the use of cloud include (i) the duration of the agreement with the date of commencement and expiry or renewal date, (ii) the service provider's responsibilities, (iii) ability of the financial institution and its external auditor to conduct audits and on-site inspections of the service provider, (iv) notification to the financial institution of adverse developments that could materially affect the service provider's ability to meet its contractual obligations, and (v) regular testing of the service provider's business continuity plans.

**4. When does cloud outsourcing fall within the scope of the rules?**

Cloud outsourcing will fall within the scope of the Outsourcing Guidelines issued by Bank Negara Malaysia, as well as the Licensing Handbook issued by the Securities Commission Malaysia, if it involves an arrangement in which a service provider performs an activity on behalf of a financial institution on a continuing basis, where the activity would otherwise be undertaken by the financial institution.

**5. Does the outsourcing need to be notified to the regulator?**

Under the Outsourcing Guidelines, a financial institution must obtain written approval from Bank Negara Malaysia before (a) entering into a new material outsourcing arrangement, or (b) making a significant modification to an existing material outsourcing arrangement. The financial institution will need to evaluate whether the arrangement is "material."

If the financial institution holds a capital markets and services license ("**CMSL Holder**"), it is only required to notify the Intermediary and Fund Supervision Division of the Securities Commission Malaysia ("**SC**") within two weeks of signing the service level agreement for any material outsourcing arrangement. In such instance, the required information for the notification is set out in the Licensing Handbook and should include the following:

A description of the material outsourced functions

An explanation of the rationale for outsourcing to the cloud service provider or subcontractor outside Malaysia and an explanation of why the specific function could not be undertaken domestically (if applicable)

A letter of undertaking is also required from the cloud service provider or subcontractor. The undertaking must state that the SC, stock exchange, derivative exchange and their agents will have access to all information, records and documents relating to the material outsourced arrangement(s). The letter of undertaking must be attached to the notification form.

The CMSL Holder must continue to notify the SC of any variation or termination of the contract with the service provider for the material outsourcing arrangement, or any adverse development arising in relation to the outsourcing arrangement of any outsourced function that could have a significant impact on the CMSL Holder within two weeks from the occurrence of the event.

**6. What are the potential consequences for breaching the financial services rules on cloud outsourcing?**

Under the Financial Services Act 2013 ("**FSA**"), Bank Negara Malaysia ("**BNM**") may issue a direction in writing if it believes that a financial institution, its director, chief executive officer or senior officer has, among other things, breached or contravened any provision of the FSA or any standards or direction issued under the FSA (this includes the guidelines issued by BNM with respect to the FSA and for the purpose of carrying out the regulatory objectives of the FSA). An institution, its director, chief executive officer or senior officer that fails to comply with such direction commits an offense and will, on conviction, be liable to imprisonment for a term not exceeding 10 years, a fine not exceeding MYR 50 million or both.

Based on the Licensing Handbook, the Securities Commission Malaysia ("**SC**") can institute an action against any person contravening the requirements specified in the Licensing Handbook, including administrative actions against capital markets services license holders as provided under the Capital Markets and Services Act 2007 ("**CMSA**"). Under the CMSA, where a person contravenes or fails to give effect to the Licensing Handbook issued by the SC, the SC may take any one or more of the actions set out below:

Direct the person in breach to comply with any requirement of the Licensing Handbook.

Impose a penalty in proportion to the severity or gravity of the breach on the person in breach, but which in any event should not exceed MYR 1 million.

Reprimand the person in breach.

Require the person in breach to remedy the breach or to mitigate its effect, including making restitution.

**7. Are there any data privacy and/or data security laws that would apply?**

Yes. The Personal Data Protection Act 2010 ("**PDPA**") governs the processing of personal data (which is defined broadly to include collecting, recording, holding, storing or carrying out any operations on personal data) in commercial transactions in Malaysia. Note, however, that the PDPA only imposes direct obligations in respect of the processing of personal data by data users. There is no provision under the PDPA that imposes a direct obligation for data processors to comply with the PDPA.

Where the cloud service providers are merely data processors that carry out data processing activities on behalf of the financial institutions (i.e., the data users), the PDPA requires the data users (in addition to other compliance obligations under the PDPA) to ensure that its data processors do the following:

Provide sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out.

Take reasonable steps to ensure compliance with those measures.

Comply with the security standards prescribed under the Personal Data Protection Standard 2015 ("**Standards**"). This relates to the security-related Standards in respect of processing personal data electronically.

In addition to the above, the following five amendments to the PDPA were expected to be tabled in Parliament in October 2022:

The requirement for data users to appoint a data protection officer

Mandatory data breach notification

Data processors being obligated to comply with the security principle under the MY PDPA

Introduction of data portability

Introduction of blacklisted countries such that transfers of personal data to these countries will be prohibited

(collectively, "**2022 Proposals**").

However, the 2022 Proposals were put on hold following the dissolution of the Malaysian Parliament in October 2022. In 2023, the new minister of communications and digital announced that the Malaysian Personal Data Protection Department is looking to enhance the 2022 Proposals before tabling the same in Parliament (the timeline of which has not been announced).

**8. Are there any restrictions under local data protection laws that would impact the overseas hosting of data?**

Yes. The Personal Data Protection Act 2010 ("**PDPA**") prohibits the transfer of personal data outside Malaysia, unless that jurisdiction has been specified by the new minister of communications and digital ("**Minister**") and published in the Gazette. To date, the Minister has yet to specify any country to which personal data may be transferred without any restrictions. Note, that there have been proposals to replace the current white-list regime with a blacklist regime (i.e., data users will generally be allowed to transfer personal data to any jurisdiction save for those blacklisted by the Minister). However, this has not yet been implemented.

Subject to further updates, it is generally recommended that data users obtain data subjects' consent prior to any cross-border transfers, as consent is one of the exceptions to the prohibition. Where it is impractical to obtain consent, data users may choose to rely on other exceptions under the PDPA, such as the following:

Where the transfer is necessary to (i) perform a contract between the data subject and the data user, or (ii) conclude or perform a contract between the data user and a third party that (A) is entered into at the data subject's request, or (B) is in the data subject's interests

Where data users have taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner that, if that place is Malaysia, would be a contravention of the PDPA

**9. Does a cloud service provider need a financial services authorization or license to provide cloud services?**

No.

**10. Is express consent from customers or other data subjects required before moving data to the cloud?**

Yes, consent from data subjects is required for the data users to move their personal data to cloud servers located outside of Malaysia. Further, the data subjects' consent is also required if the data users intend to disclose their personal data to vendors, including cloud service providers.

Where sensitive personal data is involved, the data subjects' explicit consent must be obtained. Explicit consent for sensitive personal data is not defined under the Personal Data Protection Act 2010 ("**PDPA**"), and neither is the mode of obtaining such consent. However, it is **typically construed to mean an affirmative action taken by the data subject to indicate consent** (e.g., requiring the data subject to check a box on an online form consenting to their personal data being processed in accordance with the general terms and conditions or privacy policy would be explicit consent).

Where nonsensitive personal data is involved, such consent may be in the form of implied consent or consent in the general terms and conditions used with customers, but the consent must be as follows:

(i) In a form that can be recorded and properly maintained by the data user

(ii) Presented in a distinguishable way in its appearance from another matter, if the form in which such consent is to be given also concerns another matter

Note that data subjects are also afforded the right under the PDPA to withdraw their consent to the processing of their personal data by providing a written notice in writing to the data user. Failure to comply with such request is an offense under the PDPA. Upon conviction, the data user may be liable to a fine not exceeding MYR 100,000 (approximately USD 22,500) and/or imprisonment for a term not exceeding one year.

**11. Are there any local laws that require a cloud service provider to be able to access the data it hosts?**

Yes. Licensed cloud service providers are required to comply with any lawful interception requests from the regulatory authorities. See below for further details:

The Communications and Multimedia Act ("**CMA**") provides the following:

The Malaysian communications and multimedia minister ("**Minister**") may require a licensee (which may include the cloud services provider if it is regulated as a licensed cloud service provider under the CMA) to effect an authorized interception of communications.

The Yang di-Pertuan Agong (or the Minister on his behalf) may order the interception of any communications to or from any licensee, person or the general public relating to any specified subject, on the occurrence of any public emergency or in the interest of public safety.

Under the Criminal Procedure Code, the Malaysian attorney general can require a communications service provider (such as the cloud services provider) to intercept and retain a communication received or transmitted by that communications service provider if the communication is considered likely to contain any information relating to the commission of an offence.

From a practical enforcement perspective, if the cloud service provider is (i) an offshore entity, and (ii) not a licensee under the CMA, it is unlikely that the Malaysian law enforcement authorities would expend resources to bring enforcement actions against entities outside of Malaysia.

**12. Are there any local laws that would require a cloud service provider to disclose the data it hosts to any third parties in any circumstances (including regulatory or law enforcement authorities)?**

Yes, disclosure can be required under, amongst others, the Communications and Multimedia Act, the Criminal Procedure Code and the Personal Data Protection Act 2010. Local enforcement authorities are also generally empowered under statutes to demand access to and disclosure of any data (including personal data) in carrying out lawful searches.

It is also a requirement under the Licensing Handbook for the cloud service provider and any subcontractor to issue a letter of undertaking to the Securities Commission Malaysia ("**SC**") stating that the SC, stock exchange, derivative exchange and their agents will have access to all information, records and documents relating to the material outsourced arrangement.

# Permissibility of cloud

## 1. Are financial institutions legally permitted to use cloud services?

Yes, subject to compliance with the applicable guidelines, rules, directives and guidance issued by the Securities Commission Malaysia and Bank Negara Malaysia.

# Rules for cloud outsourcing

## 2. Are there any rules that apply to cloud use by financial institutions (e.g., rules regarding outsourcing or the use of cloud services)?

Yes. The Risk Management in Technology Guidelines issued by Bank Negara Malaysia ("**BNM**") provide the following:

A financial institution must conduct a comprehensive risk assessment prior to cloud adoption. The risk assessment must consider the inherent architecture of cloud services that leverages on the sharing of resources and services across multiple tenants over the internet. The risk assessment must be documented and made available for BNM's review as and when requested.

A financial institution must notify BNM of its intention to use cloud services for noncritical systems.

A financial institution is required to consult BNM prior to using public cloud for critical systems.

A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorized disclosure and access.

Where the use of cloud services constitutes outsourcing, the financial institution must conduct appropriate due diligence of a service provider when considering all new arrangements, and when renewing or renegotiating existing arrangements.

Further, where the financial institution is a holder of a capital markets and services license ("**CMSL Holder**"), the Licensing Handbook issued by the Securities Commission Malaysia provides that a CMSL Holder is not allowed to outsource any back office function that involves (i) the financial institution's decision-making functions or (ii) any interaction or direct contact with the financial institution's clients. Therefore, where the provision of cloud outsourcing services does not involve (i) or (ii), it will be permissible for the financial institution to outsource using those cloud services.

# Contract requirements

## 3. Are there any specific contractual requirements for cloud outsourcing?

Under the Risk Management in Technology Guidelines, a financial institution must establish service level agreements when engaging third-party service providers (e.g., cloud services providers). These must be regularly reviewed to take into account the latest security and technological developments in relation to the services provided. The service level agreement should contain the following:

Access rights for the regulator and any party appointed by the financial institution to examine any activity or entity of the financial institution

Requirements for the service provider to provide sufficient prior notice to financial institutions of any subcontracting that is substantial

A written undertaking by the service provider on compliance with secrecy provisions under relevant legislation

Arrangements for disaster recovery and backup capability, where applicable

Critical system availability

Arrangements to secure business continuity in the event the service provider exits or is terminated

Other terms that are to be included in an outsourcing arrangement arising through the use of cloud include (i) the duration of the agreement with the date of commencement and expiry or renewal date, (ii) the service provider's responsibilities, (iii) ability of the financial institution and its external auditor to conduct audits and on-site inspections of the service provider, (iv) notification to the financial institution of adverse developments that could materially affect the service provider's ability to meet its contractual obligations, and (v) regular testing of the service provider's business continuity plans.

# Regulated cloud outsourcing

## 4. When does cloud outsourcing fall within the scope of the rules?

Cloud outsourcing will fall within the scope of the Outsourcing Guidelines issued by Bank Negara Malaysia, as well as the Licensing Handbook issued by the Securities Commission Malaysia, if it involves an arrangement in which a service provider performs an activity on behalf of a financial institution on a continuing basis, where the activity would otherwise be undertaken by the financial institution.

# Regulatory notifications

## 5. Does the outsourcing need to be notified to the regulator?

Under the Outsourcing Guidelines, a financial institution must obtain written approval from Bank Negara Malaysia before (a) entering into a new material outsourcing arrangement, or (b) making a significant modification to an existing material outsourcing arrangement. The financial institution will need to evaluate whether the arrangement is "material."

If the financial institution holds a capital markets and services license ("**CMSL Holder**"), it is only required to notify the Intermediary and Fund Supervision Division of the Securities Commission Malaysia ("**SC**") within two weeks of signing the service level agreement for any material outsourcing arrangement. In such instance, the required information for the notification is set out in the Licensing Handbook and should include the following:

A description of the material outsourced functions

An explanation of the rationale for outsourcing to the cloud service provider or subcontractor outside Malaysia and an explanation of why the specific function could not be undertaken domestically (if applicable)

A letter of undertaking is also required from the cloud service provider or subcontractor. The undertaking must state that the SC, stock exchange, derivative exchange and their agents will have access to all information, records and documents relating to the material outsourced arrangement(s). The letter of undertaking must be attached to the notification form.

The CMSL Holder must continue to notify the SC of any variation or termination of the contract with the service provider for the material outsourcing arrangement, or any adverse development arising in relation to the outsourcing arrangement of any outsourced function that could have a significant impact on the CMSL Holder within two weeks from the occurrence of the event.

# Consequences of regulatory breach

## 6. What are the potential consequences for breaching financial services rules on cloud outsourcing?

Under the Financial Services Act 2013 ("**FSA**"), Bank Negara Malaysia ("**BNM**") may issue a direction in writing if it believes that a financial institution, its director, chief executive officer or senior officer has, among other things, breached or contravened any provision of the FSA or any standards or direction issued under the FSA (this includes the guidelines issued by BNM with respect to the FSA and for the purpose of carrying out the regulatory objectives of the FSA). An institution, its director, chief executive officer or senior officer that fails to comply with such direction commits an offense and will, on conviction, be liable to imprisonment for a term not exceeding 10 years, a fine not exceeding MYR 50 million or both.

Based on the Licensing Handbook, the Securities Commission Malaysia ("**SC**") can institute an action against any person contravening the requirements specified in the Licensing Handbook, including administrative actions against capital markets services license holders as provided under the Capital Markets and Services Act 2007 ("**CMSA**"). Under the CMSA, where a person contravenes or fails to give effect to the Licensing Handbook issued by the SC, the SC may take any one or more of the actions set out below:

Direct the person in breach to comply with any requirement of the Licensing Handbook.

Impose a penalty in proportion to the severity or gravity of the breach on the person in breach, but which in any event should not exceed MYR 1 million.

Reprimand the person in breach.

Require the person in breach to remedy the breach or to mitigate its effect, including making restitution.

# Data privacy and security

## 7. Are there any data privacy and/or data security laws that would apply?

Yes. The Personal Data Protection Act 2010 ("**PDPA**") governs the processing of personal data (which is defined broadly to include collecting, recording, holding, storing or carrying out any operations on personal data) in commercial transactions in Malaysia. Note, however, that the PDPA only imposes direct obligations in respect of the processing of personal data by data users. There is no provision under the PDPA that imposes a direct obligation for data processors to comply with the PDPA.

Where the cloud service providers are merely data processors that carry out data processing activities on behalf of the financial institutions (i.e., the data users), the PDPA requires the data users (in addition to other compliance obligations under the PDPA) to ensure that its data processors do the following:

Provide sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out.

Take reasonable steps to ensure compliance with those measures.

Comply with the security standards prescribed under the Personal Data Protection Standard 2015 ("**Standards**"). This relates to the security-related Standards in respect of processing personal data electronically.

In addition to the above, the following five amendments to the PDPA were expected to be tabled in Parliament in October 2022:

The requirement for data users to appoint a data protection officer

Mandatory data breach notification

Data processors being obligated to comply with the security principle under the MY PDPA

Introduction of data portability

Introduction of blacklisted countries such that transfers of personal data to these countries will be prohibited

(collectively, "**2022 Proposals**").

However, the 2022 Proposals were put on hold following the dissolution of the Malaysian Parliament in October 2022. In 2023, the new minister of communications and digital announced that the Malaysian Personal Data Protection Department is looking to enhance the 2022 Proposals before tabling the same in Parliament (the timeline of which has not been announced).

# Overseas hosting

## 8. Are there any restrictions under local data protection laws that would impact the overseas hosting of data?

Yes. The Personal Data Protection Act 2010 ("**PDPA**") prohibits the transfer of personal data outside Malaysia, unless that jurisdiction has been specified by the new minister of communications and digital ("**Minister**") and published in the Gazette. To date, the Minister has yet to specify any country to which personal data may be transferred without any restrictions. Note, that there have been proposals to replace the current white-list regime with a blacklist regime (i.e., data users will generally be allowed to transfer personal data to any jurisdiction save for those blacklisted by the Minister). However, this has not yet been implemented.

Subject to further updates, it is generally recommended that data users obtain data subjects' consent prior to any cross-border transfers, as consent is one of the exceptions to the prohibition. Where it is impractical to obtain consent, data users may choose to rely on other exceptions under the PDPA, such as the following:

Where the transfer is necessary to (i) perform a contract between the data subject and the data user, or (ii) conclude or perform a contract between the data user and a third party that (A) is entered into at the data subject's request, or (B) is in the data subject's interests

Where data users have taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner that, if that place is Malaysia, would be a contravention of the PDPA

# Financial services authorizations licenses

## 9. Does a cloud service provider need a financial services authorization or license to provide cloud services?

No.

# Customer data subject consent

## 10. Is express consent from customers or other data subjects required before moving data to the cloud?

Yes, consent from data subjects is required for the data users to move their personal data to cloud servers located outside of Malaysia. Further, the data subjects' consent is also required if the data users intend to disclose their personal data to vendors, including cloud service providers.

Where sensitive personal data is involved, the data subjects' explicit consent must be obtained. Explicit consent for sensitive personal data is not defined under the Personal Data Protection Act 2010 ("**PDPA**"), and neither is the mode of obtaining such consent. However, it is **typically construed to mean an affirmative action taken by the data subject to indicate consent** (e.g., requiring the data subject to check a box on an online form consenting to their personal data being processed in accordance with the general terms and conditions or privacy policy would be explicit consent).

Where nonsensitive personal data is involved, such consent may be in the form of implied consent or consent in the general terms and conditions used with customers, but the consent must be as follows:

(i) In a form that can be recorded and properly maintained by the data user

(ii) Presented in a distinguishable way in its appearance from another matter, if the form in which such consent is to be given also concerns another matter

Note that data subjects are also afforded the right under the PDPA to withdraw their consent to the processing of their personal data by providing a written notice in writing to the data user. Failure to comply with such request is an offense under the PDPA. Upon conviction, the data user may be liable to a fine not exceeding MYR 100,000 (approximately USD 22,500) and/or imprisonment for a term not exceeding one year.

# Data access requirements

## 11. Are there any local laws that require a cloud service provider to be able to access the data it hosts?

Yes. Licensed cloud service providers are required to comply with any lawful interception requests from the regulatory authorities. See below for further details:

The Communications and Multimedia Act ("**CMA**") provides the following:

The Malaysian communications and multimedia minister ("**Minister**") may require a licensee (which may include the cloud services provider if it is regulated as a licensed cloud service provider under the CMA) to effect an authorized interception of communications.

The Yang di-Pertuan Agong (or the Minister on his behalf) may order the interception of any communications to or from any licensee, person or the general public relating to any specified subject, on the occurrence of any public emergency or in the interest of public safety.

Under the Criminal Procedure Code, the Malaysian attorney general can require a communications service provider (such as the cloud services provider) to intercept and retain a communication received or transmitted by that communications service provider if the communication is considered likely to contain any information relating to the commission of an offence.

From a practical enforcement perspective, if the cloud service provider is (i) an offshore entity, and (ii) not a licensee under the CMA, it is unlikely that the Malaysian law enforcement authorities would expend resources to bring enforcement actions against entities outside of Malaysia.

# Data disclosure requirements

## 12. Are there any local laws that would require a cloud service provider to disclose the data it hosts to any third parties in any circumstances (including regulatory or law enforcement authorities)?

Yes, disclosure can be required under, amongst others, the Communications and Multimedia Act, the Criminal Procedure Code and the Personal Data Protection Act 2010. Local enforcement authorities are also generally empowered under statutes to demand access to and disclosure of any data (including personal data) in carrying out lawful searches.

It is also a requirement under the Licensing Handbook for the cloud service provider and any subcontractor to issue a letter of undertaking to the Securities Commission Malaysia ("**SC**") stating that the SC, stock exchange, derivative exchange and their agents will have access to all information, records and documents relating to the material outsourced arrangement.

©Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership**: This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion**: All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising**: This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction**: Reproduction or copying of the Content on this Site without express written authorization is strictly prohibited.