Global Data and Cyber Handbook - Bahrain

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

# What's new?

## Recently Updated Topics

The Kingdom of Bahrain issued its first national personal data protection law on 19 July 2019 with a view to establishing the rights and freedoms of individuals and their personal data. The Law came into effect on 1 August 2019 and the Ministry of Justice, Islamic Affairs and Waqf was designated by Royal Decree in 2019 to assume the duties of the Personal Data Protection Authority. In 2022, the Ministry issued ten executive orders relating to various aspects of the Law and its implementation.

# Key Data & Cyber Contacts

# Key Data & Cybersecurity Laws

## How are data and cybersecurity laws/regulations implemented?

*Last review date: 31 December 2024*

omnibus – all personal data

sector-specific

constitutional

## What are the key data privacy laws and regulations?

*Last review date: 31 December 2024*

The primary laws relevant to privacy and data protection are:

Law No. 30 of 2018 on the Personal Data Protection Law (“**PDPL**”)

Ministry of Justice, Islamic Affairs and Waqf Executive Orders:

No. 42 of 2022 regarding the transfer of personal data outside the Kingdom of Bahrain

No. 43 of 2022 regarding the conditions to be met in the technical and organizational measures that guarantee protection of personal data

No. 44 of 2022 regarding the rules and procedures for submitting notifications and prior authorization requests to the Personal Data Protection Authority

No. 45 of 2022 regarding the rules and procedures for processing sensitive personal data

No. 46 of 2022 regarding Data Protection Guardians

No. 47 of 2022 determining the fees of enrollment and renewal in the Data Protection Guardians register and cases of waiver and refund

No. 48 of 2022 regarding the Data Subject’s Rights

No. 49 of 2022 with respect to rules and procedures governing submission of complaints regarding violations of the Personal Data Protection Law

No. 50 of 2022 determining the controls and safeguards for protecting the confidentiality of data concerning instituting and pursuing of criminal proceedings, and related judgements

No. 51 of 2022 regarding the conditions to be met while creating registers accessible to the public

## What are the key cybersecurity laws and regulations?

*Last review date: 31 December 2024*

Cybersecurity is a fundamental pillar of the national ICT framework in the Kingdom of Bahrain. The Kingdom has a national cybersecurity framework governed by the General Directorate of Anti-Corruption and Economic and Electronic Security at the Ministry of Interior that addresses cybersecurity in sectors including energy, finance, education and health.

In addition to the security-related provisions in the PDPL and its Executive Orders, the primary laws relevant to cybersecurity include:

Law No. 16 of 2014 regarding the Protection of Information and State Documents

Law No. 2 of 2017 for Ratifying the Arab Agreement on Combating IT Crimes

Law No. 60 of 2014 regarding IT Crimes

Decree-Law No. 54 of 2018 for Issuance of Letters and Electronic Transactions

Prime Ministerial Decree No. 36 of 2018 regulating the technical requirements for sending, receiving, and updating the electronic records and signatures of public bodies

## What are the key laws and regulations relating to non-personal data?

*Last review date: 31 December 2024*

Law No. 16 of 2014 regarding the Protection of Information and State Documents: This law mandates the protection of sensitive information and state documents, ensuring their security and confidentiality.

Law No. 2 of 2017 for Ratifying the Arab Agreement on Combating IT Crimes: This law focuses on combating various forms of IT crimes, including those involving non-personal data.

Law No. 60 of 2014 regarding IT Crimes: This law addresses offenses related to information technology, including unauthorized access and data breaches involving non-personal data.

Decree-Law No. 54 of 2018 for Issuance of Letters and Electronic Transactions: This law regulates electronic transactions, ensuring their security and integrity, which is crucial for the protection of non-personal data.

Prime Ministerial Decree No. 36 of 2018: This decree sets technical requirements for sending, receiving, and updating electronic records and signatures of public bodies, which includes non-personal data.

## Are new or material changes to those key data and cybersecurity laws anticipated in the near future?

*Last review date: 31 December 2024*

No imminent changes to the PDPL or core cybersecurity laws are anticipated. However, in early 2024, it was reported that the Shura Council had approved a proposal on a draft law relating to artificial intelligence that would include a new authority to regulate AI, penalties for breaches, and compensation for damages caused by AI systems.

# Regulators, Enforcement Priorities and Penalties

## Who are the main data privacy, non-personal data and/or cybersecurity regulator(s) in the jurisdiction?

*Last review date: 31 December 2024*

The Ministry of Justice, Islamic Affairs and Waqf was designated by Royal Decree in 2019 to assume the duties of the Personal Data Protection Authority (“**PDPA**”) under the PDPL.

The Kingdom’s national cybersecurity framework is overseen by the General Directorate of Anti-Corruption and Economic and Electronic Security at the Ministry of Interior (“**MoI**”) and the National Cyber Security Center.

In August 2024, and pursuant to Royal Decree No. 30 of 2024, the National Cyber Security Center was moved to fall under the supervision of the Supreme Council for Defence.

## How active is each of the regulator(s)?

*Last review date: 31 December 2024*

Moderately active

## What are each of the regulator's anticipated enforcement priorities for the next 12 months?

*Last review date: 31 December 2024*

It is anticipated that the PDPA will continue its awareness-raising, monitoring and gradual enforcement of the PDPL.

The MoI will continue to focus on cybersecurity issues, particularly in relation to cybercrime, while the National Cyber Security Center will focus on matters of strategy and national security.

## What trends are you seeing in regulatory investigations relating to data & cyber?

*Last review date: 31 December 2024*

Regulatory investigations or direct enforcement activity by data or cyber regulators are:

Rare

Class actions/group actions under data or cyber regulation are:

Rare

## What are the potential penalties/remedies for non-compliance with the key data and cybersecurity laws in the jurisdiction?

*Last review date: 31 December 2024*

**There are:**

administrative remedies / civil penalties applied by regulators and law enforcement

criminal penalties from regulators and law enforcement

private remedies

## If data subjects have private remedies, what form can these remedies take?

*Last review date: 31 December 2024*

Individual personal actions

# Key Definitions

## Personal data

*Last review date: 31 December 2024*

**Personal Data Protection Law:** Personal Data means any information in any form concerning an identified individual, or an individual who can, directly or indirectly, be identified by reference, in particular, to his or her personal identification number, or by reference to one or more factors specific to his or her physical, physiological, intellectual, cultural, economic, or social identity. In determining whether an individual is identifiable, all the means that the data controller or any other person uses or may have access to should be taken into consideration.

## Sensitive/special personal data (including personal data subject to additional protections/ restrictions/breach notification obligations)

*Last review date: 31 December 2024*

Sensitive data includes:

personal data revealing racial or ethnic origin

personal data revealing political opinions

personal data revealing religious or philosophical belief

personal data revealing trade / professional union or association membership

data concerning health/medical information

data concerning a natural person's sex life or sexual orientation

personal data regarding an individual's criminal convictions or record

## Controller vs Processor

*Last review date: 31 December 2024*

Do the privacy laws distinguish between controllers/owners and processors/agents? Whereby:

the controller/owner is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

the processor/agent is natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

Yes

# Territorial Scope

## What is the territorial reach of the data privacy and cybersecurity laws?

*Last review date: 31 December 2024*

applies to organizations located in the jurisdiction

other

In addition to applying to natural or legal persons resident or with a place of business in the Kingdom, the PDPL also applies to every natural or legal person not habitually resident nor maintaining a place of business in the Kingdom that processes personal data using means situated in the Kingdom, unless such means are used only for purposes of transit of data over the Kingdom’s territory.

# Legal Bases for Processing of Personal Data

## Is an identified legal basis required in order to collect or process non-sensitive personal data?

*Last review date: 31 December 2024*

Yes

The following are potential legal bases for processing personal data:

the data subject has provided consent to the processing for the identified purposes

the personal data is necessary to perform a contract with the data subject

the personal data is necessary to comply with a legal obligation

the personal data is necessary to protect the vital interests of a natural person

the personal data is necessary to fulfil a legitimate interest of the controller or third party (provided that the interest is not overridden by the data subject's privacy interests and the data subject has not made use of his/her right to object)

## Is an identified legal basis required in order to collect or process sensitive personal data?

*Last review date: 31 December 2024*

The following are potential legal bases for processing sensitive personal data:

the data subject has given consent to the processing, where consent is measured to the same standard as non-sensitive personal data

processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law

processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and further conditions

processing relates to personal data which are manifestly made public by the data subject

processing is necessary for the establishment, exercise or defense of legal claims

processing is necessary for the purposes of medicine, the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services (this legal basis might be indirectly and partially recognized via different other legal justifications for data processing, such as contractual performance, health and medication-related purposes).

other

Additional bases in the PDPL include:

processing is carried out by a competent public body to the extent necessary to carry out its legitimate duties as laid down by virtue of a law; and

processing of data relating to racial, ethnic, or religious origins where the processing is necessary for the purpose of identifying the existence or absence of equality of opportunity or treatment between members of the society of different racial or ethnic or religious origins, provided that such processing is carried out with appropriate safeguards for the rights and freedoms of data subjects as prescribed by law.

Further conditions around sensitive personal data processing are set out in Executive Order No. 45 of 2022.

## Are there special requirements that apply to the collection or processing of personal data from minors?

*Last review date: 31 December 2024*

No.

## In what circumstances do these special requirements apply?

*Last review date: 31 December 2024*

N/A

## What are the special requirements that apply to collecting or processing personal data from minors?

*Last review date: 31 December 2024*

N/A

# Information Requirements, Data Subject Rights, Accountability and Governance

## What information needs to be included in a privacy notice to data subjects?

*Last review date: 31 December 2024*

the identity and the contact details of the controller and, where applicable, of the controller's representative

the purposes of the processing for which the personal data is intended

the source from which the personal data originates, and if applicable, whether it came from publicly accessible sources

the recipients or categories of recipients of the personal data, if any

the existence of data subjects' rights, such as the right to access, rectification, erasure, data portability, etc. (only required for a consent form)

whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data

other

Data subjects must also be provided with any further information that is necessary in the circumstances to ensure fair processing, including whether the personal data will be used for marketing purposes.

There are certain exceptions to the information provision requirements where data is obtained indirectly, namely where the processing is undertaken for statistical purposes or historical or scientific research (and where notification to the data subject is impossible or unusually onerous) and where processing is necessary for compliance with a legal obligation or order of the court, public prosecution, investigating judge or military prosecution.

## Do data subjects have specific privacy rights that must be operationalized?

*Last review date: 31 December 2024*

**Yes**

Data subjects have the following data privacy rights, although the specifics of the scope and conditions for each of these vary depending on the circumstances and local law:

right to rectify/correct the data subject's own personal data where inaccurate or incomplete

right to erasure of personal data

right to restrict data processing

right to object to the processing of personal data

right to withdraw consent

other

The PDPL includes rights to information, a right to be notified if personal data is being processed, and a right to object to direct marketing. Further details on data subject rights are set out in Executive Order No. 48 of 2022.

## Are there accountability and governance requirements?

*Last review date: 31 December 2024*

There are accountability and governance requirements to:

take privacy by default and design measures for all processing of personal data

Privacy by design is not referenced in the PDPL, but specified as a requirement in Executive Order No. 43 of 2022.

perform and document data protection impact assessments (DPIAs) for high-risk processing:

DPIAs are not referenced in the PDPL, but specified as a requirement in Executive Order No. 43 of 2022.

maintain a record of processing activities

implement appropriate measures to comply with data privacy and security

identify a specific individual as the data privacy contact for data subject or data protection authority inquiries

provide training to employees

Training of employees is not referenced in the PDPL, but specified as a requirement in Executive Order No. 43 of 2022.

audit or supervise data processors

appoint a local representative in the jurisdiction (if the controller or processor is not located in the jurisdiction)

# DPOs and Notification Requirements

## Is the concept of data protection officer (DPO) recognized in the jurisdiction?

*Last review date: 31 December 2024*

Yes

The PDPL establishes the concept of Data Protection Guardians, which are parties accredited by and registered with the PDPA that must be appointed by controllers in certain circumstances. These may be internal (employed) or external (third party) persons meeting specific criteria set out in Executive Order No. 46 of 2022 and enrolled on the register per Executive Order No. 47 of 2022.

## Are there circumstances in which it is mandatory to appoint a DPO or similar position?

*Last review date: 31 December 2024*

Yes

If yes, under what circumstances?

The PDPA may determine specific categories of controller that are required to appoint external or internal data guardians from time to time.

## Where a DPO is appointed, does the DPO have to meet specific requirements?

*Last review date: 31 December 2024*

Yes

## Are there obligations to notify, submit filings to, register with or obtain approval from local data protection authorities to collect and/or process personal data generally?

*Last review date: 31 December 2024*

Yes

In addition to a general notification requirement, the following operations require the prior written authorization of the PDPA:

automatic processing of sensitive personal data;

automatic processing of biometric data necessary for the verification of an individual’s identity;

automatic processing of genetic data , unless carried out by physicians, or a specialist within a licensed medical establishment, and is necessary for preventative medicine, medical diagnosis or the administration of health care or treatment;

automatic processing involving linkage between personal data files, of two or more data controllers, processed for different purposes; and

processing that is done by means of visual recording, and used for surveillance purposes.

Executive Order No. 44 of 2022 provides further guidance on the rules and procedures for submitting the  various notifications and authorization requests to the PDPA as required by the PDPL.

# Data Processors

## Are there obligations for controllers to establish controls with respect to data processors?

*Last review date: 31 December 2024*

Yes

## Are there any direct regulatory or statutory requirements on processors?

*Last review date: 31 December 2024*

No

# International Data Transfer

## Are there restrictions on the transfer of personal data to third countries?

*Last review date: 31 December 2024*

Yes

Transfers of personal data to third countries are only permissible if there is a legal basis for the processing/transfer and one of the following applies:

approved adequate/whitelisted jurisdictions

other solutions

Transfers may occur if approved by the PDPA on a case-by-case basis subject to ensuring an adequate level of protection in the circumstances. Executive Order No. 42 of 2022 provides further details including the list of countries and territories that provide adequate legislative and regulatory protection as determined by the PDPA.

***Please see separate question for information on data localization provisions that are not restricted to personal data.***

# Cookies, Online Tracking and Direct Marketing

## Are there specific requirements for the use of cookies and other online tracking technologies?

*Last review date: 31 December 2024*

Yes

There is no extensive detail in the PDPL around cookies or other online tracking technologies, but Executive Order No. 48 of 2022 makes clear that a data subject’s consent is not valid if a cookie banner obliges them to provide their consent prior to accessing a website.

## Are there specific requirements related to the use of personal data for direct marketing activities?

*Last review date: 31 December 2024*

Yes

**Email marketing**

opt-out or implied consent

**Telephone marketing**

opt-out or implied consent

**SMS/text message marketing**

opt-out or implied consent

**Postal marketing**

opt-out or implied consent

**Online behavioral advertising targeting/ social media targeting/ad personalization marketing**

opt-out or implied consent

# Data Processing in the Employment Context

## Is an identified legal basis required in order to collect or process personal data or sensitive personal data in the employment context?

*Last review date: 31 December 2024*

Yes

## Can consent be validly obtained in the employment context?

*Last review date: 31 December 2024*

Yes, same as for data subjects outside the employment context.

There are no express provisions in the PDPL regarding consent in the employment context and no specific available guidance on this issue as at the end of 2024.

## Has the data privacy regulator issued guidance on use of artificial intelligence, automated decision making or profiling in an employment context – for example, relating to use in employee monitoring or hiring?

Yes

If yes, please provide a link.

[Executive Order No. 48 of 2022 on data subject rights specifies that controllers must inform subjects of decisions based on automated processing and implement clear procedures for raising objections](http://www.pdp.gov.bh/en/assets/pdf/executive-decisions/eng/Data-Subjects-Rights-REVIEWED.pdf).

# Artificial Intelligence, Profiling and Automated Decision Making

## Are there any restrictions or requirements related to creating profiles of data subjects or utilizing automated decision-making for decisions related to data subjects, including with respect to artificial intelligence?

*Last review date: 31 December 2024*

Yes

The restrictions or requirements are as follows:

 qualified right not to be subject to a decision based solely on automated decision making, including profiling – for example, only applicable if the decision produces legal effects concerning them or similarly significantly affects them

## If such restrictions or requirements exist, are they subject to any exceptions?

*Last review date: 31 December 2024*

The right does not apply where the decision is taken in the course of entering into or performance of a contract with the data subject, provided that suitable measures to safeguard his legitimate interests have been taken.

## Has the data privacy regulator issued guidance on data privacy and artificial intelligence, automated decision-making or profiling?

*Last review date: 31 December 2024*

Yes

*If yes, please provide brief details and a link.*

[Executive Order No. 48 of 2022 on data subject rights specifies that controllers must inform subjects of decisions based on automated processing and implement clear procedures for raising objections](http://www.pdp.gov.bh/en/assets/pdf/executive-decisions/eng/Data-Subjects-Rights-REVIEWED.pdf).

## Has the data privacy regulator taken enforcement action in relation to artificial intelligence, including automated decision-making or profiling?

*Last review date: 31 December 2024*

No enforcement activity to date

## Do other (non-personal data or cybersecurity) laws or regulations impose restrictions on use of artificial intelligence, automated decision-making or profiling?

*Last review date: 31 December 2024*

Proposal for legislation or regulation at an early stage

In early 2024, it was reported that the Shura Council had approved a proposal on a draft law relating to artificial intelligence that would include a new authority to regulate AI, penalties for breaches, and compensation for damages caused by AI systems.

# Data privacy and cybersecurity in a transactional context

## Has the data privacy authority issued any guidance on data privacy compliance in the context of transactional activity (including, but not limited to, share sales, asset sales, reorganizations or spinouts)?

*Last review date: 31 December 2024*

No

## In the context of an asset sale (the sale of a separate business unit as a going concern), does the acquiring entity inherit liability for pre-acquisition data privacy or cybersecurity breaches (connected with the assets that are the subject of the asset sale)?

*Last review date: 31 December 2024*

No

## If so, how would any regulatory fines be calculated?

*Last review date: 31 December 2024*

Unclear

## In the context of a share sale (where the acquiring entity acquires 100% of the shares of a target company), does the acquiring entity inherit liability for pre-acquisition data privacy or cybersecurity breaches (connected with the target company)?

*Last review date: 31 December 2024*

No

## If so, how would any regulatory fines be calculated?

*Last review date: 31 December 2024*

Unclear

# Security Requirements and Breach Notification

## Do data privacy laws or regulations impose obligations to maintain information security controls to protect personal data from unauthorized access or processing?

*Last review date: 31 December 2024*

Yes

general obligation to take appropriate / reasonable technical, physical and/or organizational security measures

requirement to undertake third party due diligence (security assessment of third party providers)

Further details on technical and organizational measures to guarantee protection of personal data are set out in Executive Order No. 43 of 2022.

## Do other laws or regulations impose obligations to protect systems from cyberattack?

*Last review date: 31 December 2024*

Yes

other

If yes, please provide brief details of the relevant law or regulation.

Law No. 16 of 2014 regarding the Protection of Information and State Documents, which mandates the protection of sensitive information and state documents.

Prime Ministerial Decree No. 36 of 2018 sets technical requirements for sending, receiving, and updating electronic records and signatures of public bodies.

## Has there been regulatory activity – including enforcement action, investigations, regulatory guidance or other public statements by the regulator – relating to cybersecurity by the following regulators in the last 12 months?

*Last review date: 31 December 2024*

**National Cyber Security Center ("NCSC"):** The NCSC has been proactive in enhancing cybersecurity awareness and education. In 2024, they launched the National Cybersecurity Awareness Campaign, which included comprehensive training programs tailored for public sector employees. These initiatives aim to bolster the overall cybersecurity posture of Bahrain by equipping individuals with the necessary skills and knowledge to combat cyber threats.

**General Directorate of Anti-Corruption and Economic and Electronic Security ("MOI"):** This directorate plays a crucial role in the implementation of Bahrain's National Cybersecurity Strategy. Their efforts are focused on safeguarding critical national infrastructure and ensuring a robust response to cyber threats.

## Does data privacy or cybersecurity law impose obligations to make notifications about personal data security breaches?

*Last review date: 31 December 2024*

Yes

The primary obligation is set out in the PDPL with supplementary requirements in Executive Order No. 43 of 2022.

## Controllers/Owners have to notify:

*Last review date: 31 December 2024*

data protection authorities

affected individuals

other

Executive Order No. 43 of 2022 requires controllers to establish communications channels with data subjects to enable them to report breaches or potential violations.

## Processors/Agents have to notify:

*Last review date: 31 December 2024*

N/A

## Are there any additional sector-specific or non-personal data security breach notification requirements?

*Last review date: 31 December 2024*

Yes

**Telecommunication requirements**

The Telecommunications Regulatory Authority (**"TRA"**) has specific guidelines for telecom operators regarding data security and breach notifications. Operators are required to report any significant data breaches that could impact the confidentiality, integrity, or availability of telecommunications services.

**Providers of critical infrastructure**

Organizations that manage critical infrastructure are subject to stringent cybersecurity requirements. They must report any cyber incidents that could compromise the security and functionality of essential services.

**Other**

The Central Bank of Bahrain (**"CBB"**) mandates that financial institutions must notify the CBB of any material data breaches. This includes breaches that could affect the financial stability or integrity of the institution.

# Data localization and regulation of non-personal data

## Are there data localization/data residency or other types of laws that may require the retention and storage of data in the local jurisdiction, or prohibit the transfer of data out of the jurisdiction?

*Last review date: 31 December 2024*

No

The PDPL does not mandate the retention and storage of personal data within the Kingdom. However, the transfer of personal data outside Bahrain is regulated. According to Executive Order No. 42 of 2022, personal data can only be transferred to countries or regions that provide adequate protection for personal data as determined by the Authority. The Authority has listed 83 countries that meet these criteria. Data controllers may transfer personal data to these countries without prior authorization. For transfers to countries not on the list, data controllers must obtain permission from the Authority, ensure the data subject has consented, or meet specific conditions such as contractual necessity or vital interest protection.

## Does law or regulation impose mandatory requirements to share or make accessible non-personal data?

*Last review date: 31 December 2024*

Obligation for public sector organizations to share or make accessible non-personal data

Bahrain Government has an Open Data Policy incorporating a commitment to making non-sensitive data more accessible and easily shareable.

## What specific obligations do these data-sharing rules impose on private organizations?

*Last review date: 31 December 2024*

N/A. The Open Data Policy applies only to the public sector.

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 of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.