DREWACADEMY
DATA PROTECTION & CYBERSECURITY SERVICES

10 THINGS TO INCLUDE IN YOUR CONTRACT FOR AN AI SOLUTION

LEGAL GUIDES 2023

CONTENTS

Developments as of 11 April 2023

10 THINGS TO INCLUDE IN YOUR CONTRACT FOR AN AI SOLUTION

With the uncertainty surrounding the issue of liability for artificial intelligence (“**AI**”) systems under existing statutes and common law, it is important that parties involved in the procurement of a custom AI system identify and protect their interests contractually, whether as procurer or provider.

An “AI system” refers to the AI model that has been selected and deployed for use, whereas an “AI model” is created when algorithms (a set of rules/instructions given to a computer for it to do a task) analyse data, leading to an output/result which is examined and the algorithms iterated until the most appropriate model emerges.[1]

This article identifies a non-exhaustive list of 10 areas for consideration by parties when entering into a contract to develop an AI solution.

Responsibilities of parties

The key stages of AI system development may generally be split into the: (a) selection and inputting of data into the AI system; (b) training, testing and usage of the AI system; (c) maintenance of the AI system (including protections from hacking and data breaches).[2] As the development of a custom AI solution is a collaborative effort, the solution procurer and provider (i.e. developer) should consider what their respective duties and responsibilities at various stages of development are in order to mitigate their legal risks and provide greater commercial certainty. The procurer should also take steps to familiarise itself with the technology (e.g. what is AI, what does it mean to train the model) and the risks so that it is in a better position to negotiate the terms and ask pertinent questions, instead of leaving it entirely in the hands of the provider.

The functioning of an AI system is dependent on the quantity and quality of the data that is inputted at various stages of its development and deployment. The right algorithm may still produce a wrong output if the data it relied on is incorrect – for example in a GPS system, where the algorithm is to give the fastest route between two points, if instead of real-time traffic data, the traffic data from the day before is inputted, changes in the traffic would mean that the algorithm gives a result that is not actually the fastest route, but the algorithm is nonetheless correct given the input it had.[3]

It is thus imperative that parties consider how data that would be used to train the AI solution will be sourced, whether from the procurer, provider, both parties jointly, or from a third party. Where the completeness, accuracy and representativeness of the data is particularly important to the operation of the AI system, parties should provide for such requirements in their contract, and have in place procedures for the maintenance of the data quality throughout the entire data lifecycle.[4] In this regard, parties should keep a record of the data used (e.g. where it came from, whether it was edited, how recent it is) and store these records for future reference. This would be in line with the recommendations of Singapore’s Companion to the Model AI Governance Framework - Implementation and Self-Assessment Guide for Organizations (see section 4), available here.

With regards to the training and testing of the algorithms underlying the AI system, the part(ies) responsible for updating data inputted into the system and correcting wrong decisions generated by the system should be identified. In this regard, the solution provider may be better placed to train (and retrain) the AI system, identify areas where correction may be needed (with input from the procurer), and conduct testing to ensure that the system generates decisions with the expected level of accuracy.

[1] See [3.20] and [3.21] of the Model Framework.
[2] This is based on the 3-stage framework used in the article by Lim, Ernest, “*B2B Artificial Intelligence Transactions: A Framework for Assessing Commercial Liability*”.
[3] See *“Trust but Verify: A Guide to Algorithms and the Law”* by Deven R. Desai and Joshua A. Kroll at pp. 24 – 25, available at: https://jolt.law.harvard.edu/assets/articlePDFs/v31/31HarvJLTech1.pdf
[4] See article “*A Comprehensive Overview Of Data Quality Monitoring*” by Stephen Oladele and Danny D. Leybzon (published 20-Apr-2022), WhyLabs, available at: https://whylabs.ai/blog/posts/a-comprehensive-overview-of-data-quality-monitoring-2

When the AI system is deployed, the part(ies) who are responsible for monitoring the AI system to ensure it continually produces acceptable output, and providing support and maintenance, should be provided for in the contract. This may usually be the role of the solution provider.

Results the AI system is to yield, and parties' expectations

It is important for the solution procurer to articulate, with the appropriate level of precision, the standard of performance that is expected of the AI solution (and the consequences for failure to meet them). Based on the expectations expressed by the procurer, the provider can demonstrate what is within its control or not, better informing the standards set so that the provider may not be held liable for outcomes that are beyond its control. For example, if the AI system must be "explainable", parties need to be clear on what that means – does it mean that each output of the AI system will be accompanied by reasons, or if the AI system is very complex, will it be sufficient to explain how it was trained and the factors that it considers?

In the same vein, it is important to set a means of verifying that the performance standards are met. For example, the results after testing the trained AI model should be discussed between the procurer and provider, so that an acceptable level of accuracy can be agreed upon. It is generally not possible to achieve 100% accuracy with an AI model, because it is trained on data that has certain characteristics where it formulates rules based on those characteristics which are then applied to data that has similar but not always identical characteristics, so it could be benchmarked against the human error rate for the same task. The procurer may also consider having a third-party to audit the developed AI system to provide the procurer with assurance that the system meets their requirements, especially where the procurer does not have the relevant technical expertise.

Caveats on the use of AI solution

The provider should be upfront about the limitations of the AI system it develops. When an AI system is trained by particular datasets, it may produce incorrect or unreliable output if it is used for subjects not covered by the dataset. The risks/limitations should be communicated to the procurer by the provider, and the procurer should sign off in writing acknowledging their receipt of such explanation.[5]

Access to documents and information

Because the procurer may receive questions from persons about its AI system (e.g. from regulators, or the procurer's customers who are affected by its use), it may be particularly important for the procurer to have access to reports and information from the provider regarding how the AI system arrives at a decision. Such information should be presented in a manner that is comprehensible to the provider (and to the person who posed the query) – so technical jargon and lines of code would not suffice. The procurer can use the materials to explain how the decision was arrived at, and reduce the risk of challenge of the decision on grounds of unreasonableness/arbitrariness. The procurer may even require (in the contract) that the provider agree to assist with answering queries from regulators, with the exact scope of this requirement (frequency, level of assistance and compensation) to be negotiated between parties.

Data recording and logging

As mentioned earlier, data logging and monitoring is a key aspect to ensuring the system is performing as expected, and for troubleshooting in the event of errors. In the event that there are unexpected outputs generated by the AI system, the data logs can be referred to for purposes such as troubleshooting or for an investigation into how the model was functioning or why a particular prediction was made.[6] It can also be used for demonstrating compliance with relevant regulatory standards and

[5] Japan Governance Guidelines for Implementation of AI Principles (ver 1.1) at p. 30.
[6] See [3.36] of Singapore's Model AI Governance Framework.

requirements. Parties may consider requiring logging of relevant data and events in the allocation of responsibilities under their agreement, and ensuring that these logs are not modified without authorisation.

Intellectual property

The ownership of intellectual property over various aspects of the AI system (including the AI algorithms and data inputs, as well as the output generated by the AI system) should be clearly provided for in the contract, especially given the collaborative nature of the development of custom AI solutions. Where the development of the system involves the use of confidential information belonging to either party, confidentiality clauses ought to also be put in place.

A key issue for consideration is the uncertainty over the state of the law regarding the ownership of AI-generated creations due to the requirement for human authors/inventors. In this regard, parties may wish to agree on identifying a person as the human author/inventor of the work, and providing in contract how ownership of IP subsisting in the work may be allocated.

Protection of personal data

An AI system may be trained on personal data, and also process personal data. The procurer may provide the provider with the personal data of its customers for the purposes of training the model, and the provider must ensure that the data is stored safely. Parties would have different obligations depending on whether they are a data controller or data intermediary under the Personal Data Protection Act 2012. It is important to ensure that the provider of the personal data has obtained the necessary consents (or is able to rely on exceptions to consent) for the personal data to be used.

Compliance with relevant regulatory requirements

Contractual terms do not preclude parties from their obligations under the law. Where the procurer intends to use the AI solution to aid, augment and/or replace its decision-making process or operations, the procurer is still required to comply with all relevant laws. Examples of such laws that may apply include, but are not limited to, personal data protection laws, intellectual property laws and sectoral regulations such as healthcare and financial regulations.

Indemnity clause

It is important that parties consider the scope of damages covered by the indemnity clause in their contract. An indemnity clause is one that allocates identified risks, by one party promising to compensate the other party for the loss it suffers when the identified risk materalises. In negotiating the terms of the clause, parties ought to consider the nature of the AI system (i.e. what it is used for) and the potential risks they are consequently exposed to. Examples of indemnity events may include damages or injury to third parties caused by defects in the AI system, and IP infringement by the provider, among other things.

Exclusion and limitation of liability clauses

When negotiating the scope of exclusion and limitation of liability clauses in the contract, parties should ensure their compliance with the standard of reasonableness imposed by the Unfair Contract Terms Act 1977 ("**UCTA**"). Section 2(2) of UCTA states that in relation to losses or damages (other than death or personal injury resulting from negligence), a person cannot so exclude or restrict his liability for negligence except in so far as the term or notice satisfies the requirement of reasonableness. This means that the term should be a fair and reasonable one, having regard to the circumstances which were, or ought reasonably to have been, known to or in the contemplation of the parties at the time the contract was made. Various factors that may go towards showing "reasonableness" by the party relying on the clause include the relative bargaining strength of the parties, availability of independent advice and industry practice.

If a party seeks to restrict liability to a specified sum, in ascertaining whether the contractual term satisfies the requirement of reasonableness, regard shall be had to: (a) the resources which he could expect to be available to him for the purpose of meeting the liability should it arise; and (b) how far it was open to him to cover himself by insurance (Section 11(4) of UCTA).

Drew Academy wishes to acknowledge our Associate See Too Hui Min for assisting in the preparation of this article.

The content of this article does not constitute legal advice and should not be relied on as such. Specific advice should be sought about your specific circumstances.

DREW DATA PROTECTION & CYBERSECURITY ACADEMY

Drew Data Protection & Cybersecurity Academy (Drew Academy) was established in 2020 by Drew & Napier to help our clients build their capabilities and develop and implement organisational strategies, structures, policies and processes to meet their legal, regulatory and compliance obligations. Drew Academy offers a range of courses in areas such as data protection, cybersecurity, data governance and in-house commercial practice. A particular focus for us is the delivery of workplace learning solutions and development of customised training courses. We also offer outsourced DPO services and data protection consulting services through our experienced team of practitioners.

Drew Academy is helmed by Lim Chong Kin and David N. Alfred. Our course leaders are experienced in various aspects of data and cyber governance, data protection, cybersecurity engineering and in-house commercial practice.

ARTIFICIAL INTELLIGENCE AND DIGITAL TRUST

Drew & Napier's Artificial Intelligence (AI) and Digital Trust practice brings together its expertise across several technology-related domains and in fields as diverse as data protection, cybersecurity, healthcare, Fintech, intellectual property and competition law (to name a few) to advise clients on the full range of legal issues relating to AI and Digital Trust. In addition to advising on commercial, regulatory and international / cross-border issues, our advice extends into areas such as governance and ethics as we seek to enable our clients to navigate areas where laws and legal principles are still emerging.

Working together with the Drew Academy, we provide solutions that reflect our deep understanding of underlying technologies, the risks and uncertainties involved and practical business considerations. Internationally, there is a growing consensus on AI governance.

For more information on our experience, please contact:

Lim Chong Kin
Managing Director, Corporate & Finance;
Co-Head, Data Protection,
Privacy & Cybersecurity Practice;
Co-Head, Drew Data Protection &
Cybersecurity Academy

T: +65 6531 4110
E: chongkin.lim@drewnapier.com

Benjamin Gaw
Director, Corporate and
Merger & Acquisitions;
Head, Healthcare & Life Sciences
(Corporate & Regulatory)

T: +65 6531 2393
E: benjamin.gaw@drewnapier.com

David N. Alfred
Director, Corporate & Finance;
Co-Head, Data Protection,
Privacy & Cybersecurity Practice;
Co-Head and Programme Director,
Drew Data Protection &
Cybersecurity Academy

T: +65 6531 2342
E: david.alfred@drewnapier.com

Cheryl Seah
Director, Corporate & Finance

T: +65 6531 4167
E: cheryl.seah@drewnapier.com

DREWACADEMY
DATA PROTECTION & CYBERSECURITY SERVICES

10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315

www.drewnapier.com/Academy

T: +65 6531 4152
F: +65 6535 4864
E: academy@drewnapier.com

In association with

DREW & NAPIER