ICCA
INTERNATIONAL COUNCIL FOR COMMERCIAL ARBITRATION

NEW YORK CITY BAR
New York City Bar Association

CPR
International Institute for Conflict Prevention & Resolution

# ICCA–NYC Bar–CPR Protocol on Cybersecurity in International Arbitration (2022 Edition)

with the assistance of the
Permanent Court of Arbitration
Peace Palace, The Hague


The ICCA Reports No. 6

INTERNATIONAL COUNCIL FOR
COMMERCIAL ARBITRATION

# ICCA – NYC BAR – CPR PROTOCOL ON CYBERSECURITY IN INTERNATIONAL ARBITRATION (2022 EDITION)

THE ICCA REPORTS NO. 6

2022

ICCA is pleased to present the ICCA Reports series in the hope that these occasional papers, prepared by ICCA interest groups and project groups, will stimulate discussion and debate.

INTERNATIONAL COUNCIL FOR
COMMERCIAL ARBITRATION

# ICCA – NYC BAR – CPR PROTOCOL ON CYBERSECURITY IN INTERNATIONAL ARBITRATION (2022 EDITION)

THE ICCA REPORTS NO. 6

2022

with the assistance of the
Permanent Court of Arbitration
Peace Palace, The Hague


www.arbitration-icca.org

Published by the International Council for Commercial Arbitration <www.arbitration-icca.org>, the New York City Bar Association <www.nycbar.org>, and the International Institute for Conflict Prevention and Resolution (CPR) <www.cpradr.org>

ISBN 978-94-92405-32-6



For further information, please contact us at bureau@arbitration-icca.org.

**All views expressed in this Report are those of the Working Group and not of CPR, NYC Bar or ICCA, or their governing bodies or members. This Report is the result of the collective efforts of the Working Group, the views expressed are not attributable to any particular Working Group member and all Working Group members served in their individual capacity.**

### About ICCA

The International Council for Commercial Arbitration (ICCA) is a worldwide non-governmental organization (NGO) devoted to the use and improving the processes of arbitration, conciliation and other forms of resolving international disputes. Its activities include convening biennial international arbitration congresses; sponsoring authoritative dispute resolution publications (including the ICCA Yearbook Commercial Arbitration, International Handbook on Commercial Arbitration and ICCA Congress Series); and promoting the harmonization of arbitration and conciliation rules, laws and standards. ICCA has official status as an NGO recognized by the United Nations. See www.arbitration-icca.org.

### About the New York City Bar Association

The New York City Bar Association (NYC Bar), founded in 1870, is a voluntary association of lawyers and law students. NYC Bar's mission is to equip and mobilize a diverse legal profession to practice with excellence, promote reform of the law, and uphold the rule of law and access to justice in support of a fair society and the public interest in our community, our nation, and throughout the world. NYC Bar continues to work to diversify its membership and to expand its involvement in access to justice initiatives, international human rights, and pro bono representation in many areas, including immigration, homelessness, and veterans assistance.

### About the International Institute for Conflict Prevention and Resolution

Established in 1977, the International Institute for Conflict Prevention and Resolution (CPR) is an independent nonprofit organization that promotes the prevention and resolution of conflict to better enable purpose through the CPR Institute and its subsidiary, CPR Dispute Resolution Services, LLC.

The CPR Institute drives and advocates for a global prevention and dispute resolution culture through the thought leadership of its diverse members – companies, leading

mediators and arbitrators, law firms, individual practitioners, and academics – who share best practices and develop innovative tools for dispute management through Committees and events.

CPR Dispute Resolution Services, LLC (DRS) is a subsidiary of CPR (also referred to herein as the CPR Institute). It is a boutique provider of leading-edge dispute management services – mediation, arbitration, custom appointing services, a panel of dispute prevention specialists, and more – that leverages resources generated by the CPR Institute. The DRS case administrators have legal degrees, a combined 50 years of experience in ADR, and speak five languages. The Panel of Distinguished Neutrals (the Panel or the Neutrals) is a carefully curated, diverse group of prominent, experienced subject matter and ADR experts based in 35 countries.

# Table of Contents

# Members of the Working Group

***ICCA Representatives***

*Chair:* **Brandon Malone**, Independent Arbitrator, Arbitra International

**Paul Cohen**, 4-5 Gray's Inn Square Chambers

**Kathleen Paisley**, International Arbitrator, Ambos Lawyers

***NYC Bar Representatives***

**Stephanie Cohen**, Independent Arbitrator

**Lea Haber Kuck**, Independent Arbitrator; Retired Partner, Skadden, Arps, Slate, Meagher & Flom LLP

**Mark Morril**, Independent Arbitrator

***CPR Representatives***

**Olivier André**, Freshfields Bruckhaus Deringer LLP

**Hagit Elul**, Hughes Hubbard & Reed LLP

**Micaela McMurrough**, Covington & Burling LLP

*Secretaries:* **Eva Y. Chan** and **Jesse R. Peters**, Skadden, Arps, Slate, Meagher & Flom LLP

# Foreword to the 2022 Protocol

## I. Purpose of the Protocol

The purpose of the ICCA-NYC Bar-CPR Cybersecurity Protocol for International Arbitration (the "**Cybersecurity Protocol**" or the **"Protocol**") is twofold.

**First**, the Protocol is intended to provide a framework to determine reasonable information security measures for individual arbitration matters. That framework includes procedural and practical guidance to assess security risks and identify available measures that may be implemented.

**Second**, the Protocol is intended to increase awareness about information security in international arbitrations. This includes awareness of: (i) information security risks in the arbitral process, which include both cybersecurity and physical security risks; (ii) the fact that reasonable information security is required by law in many jurisdictions; (iii) the importance of information security to maintaining user confidence in the overall arbitral regime; (iv) the essential role played by individuals involved in the arbitration in effective risk mitigation; and (v) some of the readily accessible information security measures available to improve everyday security practices.

## II. Scope of the Protocol

### *(a) Application Beyond International Commercial Arbitrations*

Although the Protocol has been drafted with international commercial arbitrations in mind, it may also be a useful reference for domestic arbitration matters and/or investor-state arbitrations, as well as mediations and other ADR procedures.

### *(b) Data Protection Issues*

Information security and data protection issues are closely connected, largely because there is increasing regulation around the globe governing the processing of personal data. It is typical for data protection laws and regulations to mandate, among other things, that entities and individuals processing personal data implement reasonable information security measures.

The ICCA-IBA Roadmap to Data Protection in International Arbitration (the "Roadmap") is being launched concurrently with this 2022 edition of the Protocol. The Roadmap

recognizes that adherence to the Protocol facilitates compliance with data protection legal regimes, such as the European Union General Data Protection Regulation ("**GDPR**"), which require reasonable information security. Readers may refer to the Roadmap for further guidance on the application of the data protection laws during an arbitration.

The Protocol is intended to complement the Roadmap and other resources on data protection compliance by providing guidance in the arbitration context on: (i) the mitigation of information security risks and (ii) breach notification expectations and procedures. The Protocol recognizes that breach notification is one aspect to be considered when preparing an incident response plan for situations in which information security may have been compromised, and that notice expectations and procedures warrant special attention because whether a security incident (or "data breach" under the GDPR) constitutes a security breach triggering notice obligations (often on a very short timeline) will depend on applicable law. The Protocol does not supersede applicable legal or other binding obligations, and while implementation of the Protocol supports compliance with the security requirements imposed by data protection laws, it does not impact the many other requirements imposed by those laws.

## III. Revisions to the Protocol

This 2022 edition of the Protocol was launched at the XXVth Congress of ICCA held in Edinburgh Scotland. In addition to updating the list of references found at Schedule E, the main revision from the 2020 Protocol, which was released in late 2019 and was the original iteration of the Protocol, was to add the sample personal data breach protocol found at Schedule D-1. This addition recognises the importance of having an incident response plan in place were a security incident to occur during an arbitration.

These changes reflect that the cybersecurity and data protection environment in which the Protocol operates has matured in the nearly three years since the Protocol was launched, but the general principles remain the same. In particular, the number of global cyberattacks has increased, the sophistication of cyber threat actors has evolved, and the issue of cybersecurity has received increased attention on the world stage. Entities of all kinds have matured their cybersecurity systems and processes at the same time that regulators have placed increased focus on establishing and maintaining reasonable cybersecurity practices and programs. At the same time, the arbitration community has become increasingly aware of its security obligations in the digital environment, which awareness was accelerated by the changes that occurred during the pandemic. It is against this backdrop of increased awareness and attention that we issue the 2022 edition of the Protocol.

The Working Group has adopted the editioning approach to emphasize that the Protocol will necessarily evolve over time in light of (i) changing technology; (ii) new and

prevalent cyber threats; (iii) new or amended laws/regulations; (iv) consensus that may emerge as to reasonable measures/arbitration best practices; (v) new cybersecurity initiatives by institutions or others; and (vi) practical experience implementing the Protocol. To facilitate the periodic improvement and updating of the Protocol, the Working Group encourages persons who use the Protocol to share their experiences in deploying it and provide feedback. Feedback on the Protocol may be sent to cybersecurity@arbitration-icca.org.

For an electronic copy of the Protocol with hyperlinks and bookmarks to facilitate navigation, please visit: https://www.arbitration-icca.org/projects/Cybersecurity-in-International-Arbitration.html.

# ICCA-NYC BAR-CPR CYBERSECURITY PROTOCOL FOR INTERNATIONAL ARBITRATION (2022) (Without Commentary)

## *Scope and Applicability*

**Principle 1** The Cybersecurity Protocol provides a recommended framework to guide tribunals, parties, and administering institutions in their consideration of what information security measures are reasonable to apply to a particular arbitration matter.

**Principle 2** As a threshold matter, each party, arbitrator, and administering institution should consider the baseline information security practices that are addressed in Schedule A and the impact of their own information security practices on the arbitration. Effective information security in a particular arbitration requires all custodians of arbitration-related information to adopt reasonable information security practices.

**Principle 3** Parties, arbitrators, and administering institutions should ensure that all persons directly or indirectly involved in an arbitration on their behalf are aware of, and follow, any information security measures adopted in a proceeding, as well as the potential impact of any security incidents.

**Principle 4** The Protocol does not supersede applicable law, arbitration rules, professional or ethical obligations, or other binding obligations.

## *The Standard*

**Principle 5** Subject to Principle 4, the information security measures adopted for the arbitration shall be those that are reasonable in the circumstances of the case as considered in Principles 6–8.

## *Determining Reasonable Cybersecurity Measures*

**Principle 6** In determining which specific information security measures are reasonable for a particular arbitration, the parties and the tribunal should consider:

(a) the risk profile of the arbitration, taking into account the factors set forth in Schedule B;
(b) the existing information security practices, infrastructure, and capabilities of the parties, arbitrators, and any administering institution, and the extent to

which those practices address the categories of information security measures referenced in Principle 7;
(c) the burden, costs, and the relative resources of the parties, arbitrators, and any administering institution;
(d) proportionality relative to the size, value, and risk profile of the dispute and, where data protection laws and regulations apply, to the impact on the data subject; and
(e) the efficiency of the arbitral process.

**Principle 7** In considering the specific information security measures to be applied in an arbitration, consideration should be given to the following categories:

(a) asset management;
(b) access controls;
(c) encryption;
(d) communications security;
(e) physical and environmental security;
(f) operations security; and
(g) information security incident management, including breach notification expectations and procedures.

**Principle 8** In some cases, it may be reasonable to tailor the information security measures applied to the arbitration to the risks present in different aspects of the arbitration, which may include:

(a) information exchanges and transmission of arbitration-related information;
(b) storage of arbitration-related information;
(c) travel;
(d) hearings and conferences, whether in-person or fully or partially remote; and/or
(e) post-arbitration retention and destruction policies.

## *The Process to Establish Reasonable Cybersecurity Measures*

**Principle 9** Taking into consideration the factors outlined in Principles 6–8 as appropriate, the parties should attempt in the first instance to agree on reasonable information security measures.

**Principle 10** Information security should be raised as early as practicable in the arbitration, which ordinarily will not be later than the first case management conference.

**Principle 11** Taking into consideration Principles 4–9 as appropriate, the arbitral tribunal has the authority to determine the information security measures applicable to the arbitration.

**Principle 12** The arbitral tribunal may modify the measures previously established for the arbitration, at the request of any party or on the tribunal's own initiative, in light of the evolving circumstances of the case.

**Principle 13** In the event of a breach of the information security measures adopted for an arbitration proceeding or the occurrence of an information security incident, the arbitral tribunal may, in its discretion: (a) allocate related costs among the parties; and/or (b) impose sanctions on the parties.

**Principle 14** The Protocol does not establish any liability or any liability standard for any purpose, including, but not limited to, legal or regulatory purposes, liability in contract, professional malpractice, or negligence.

# ICCA-NYC BAR-CPR CYBERSECURITY PROTOCOL FOR INTERNATIONAL ARBITRATION (2022) (With Commentary)

## Organization of the Protocol

The Protocol is organized into Principles, Commentary, and Schedules. Each Principle provides high-level guidance and is accompanied by explanatory Commentary. The Principles are supplemented as necessary with more detailed guidance contained in the Schedules. Following the Schedules, the Working Group acknowledges the many organizations and individuals who contributed to the Protocol.

- **Principles 1–4** address the scope and applicability of the Protocol.
  - **Principle 1** establishes the basic building blocks of the Protocol, including the framework approach and the reasonableness standard.
  - **Principles 2–3** address the role of the arbitral tribunal,[1] the parties[2] and any administering institution[3] in ensuring effective information security[4] for a particular arbitration matter.
  - **Principle 4** addresses the relationship between the Protocol and applicable law and other binding obligations.
- **Principle 5** establishes the standard of reasonableness, which governs what measures should be adopted to address issues of information security in an individual arbitration matter.

1. "**Arbitral tribunal**" or "**tribunal**" refers to a sole arbitrator or a panel of arbitrators.
2. "**Party**" or "**parties**" refers to the parties to the arbitration and their counsel or other representatives.
3. "**Administering institution**" or "**institution**" refers to any institution administering the arbitration and the individual representatives of the institution.
4. "**Information security**" includes security for all types and forms of electronic and non-electronic information, including both commercial and personal data, as well as breach notification procedures and other incident response measures. "**Cybersecurity**," which concerns the means employed to maintain the confidentiality, integrity, and availability of digital information, is one aspect of information security.

- **Principles 6–8** set out a series of factors to be considered in determining what information security measures are reasonable in a particular matter and how they should be applied.

- **Principles 9–13** provide a series of suggested procedural steps to address information security issues in an individual arbitration.

  - **Principles 9–10** recognize the importance of party autonomy in determining what information security measures are reasonable in any given case.
  - **Principles 11–13** recognize the arbitral tribunal's authority to determine the information security measures applicable to the arbitration.

- **Principle 14** clarifies that the Protocol does not establish liability or a liability standard for any purpose whatsoever.

- **Schedule A** addresses baseline information security practices that all custodians of arbitration-related information should consider in connection with their everyday business activities.

- **Schedule B** considers the risk factors that can be used to assess the risk profile of an arbitration.

- **Schedule C** gives examples of specific information security measures and processes that might be adopted for particular arbitration matters.

- **Schedule D** contains sample language for addressing information security issues in arbitration agreements, agendas for case management conferences, procedural orders, and post-arbitration dispute resolution clauses.

- **Schedule D-1** supplements Schedule D with sample language for a GDPR personal data breach protocol.

- **Schedule E** lists prevailing cybersecurity standards and resources that may be consulted for further information.

- **Schedule F** is a glossary of terms used in the Protocol, which are also included in footnotes for ease of use.

## Scope and Applicability

**1** **The Cybersecurity Protocol provides a recommended framework to guide tribunals, parties, and administering institutions in their consideration of what information security measures are reasonable to apply to a particular arbitration matter.**

***Commentary to Principle 1***

(a) ***Recommended framework.*** Principle 1 establishes the basic approach of the Protocol, which is to provide a framework for the consideration of the security measures to be applied to the information processed[5] during a particular arbitration matter.

(b) The Protocol is not intended to, and does not, provide a one-size-fits-all information security solution. A core premise of the Protocol is that reasonable information security measures should be applied to arbitral proceedings, but that the measures that will be reasonable in a particular matter may vary significantly based on the facts and circumstances of the case, as well as evolving threats and technology. Tribunals and parties who decide to utilize the Protocol in an arbitration can refer to the guidance in the Protocol to determine reasonable information security measures for their matter.

(c) ***Relationship between cybersecurity and information security.*** Due to the highly digitized nature of today's international arbitrations, the Protocol focuses on cybersecurity, which concerns the means employed to maintain the confidentiality, integrity, and availability of digital information.[6] However, the guidance in the Protocol applies broadly to all information security measures, including both cybersecurity and physical security, and the Protocol therefore refers generally to information security rather than to cybersecurity wherever appropriate. As such, in this Protocol, the term "information security" includes security for all types and

5. "**Processing**" broadly refers to anything that is done to, or with, arbitration-related information. It includes automated and non-automated operations, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment or combination, restriction, erasure, or destruction.
6. In this context, "**confidentiality**" can be understood as a set of rules or restrictions that limits access to certain information, "**integrity**" can be understood as an assurance that certain information is trustworthy and accurate, and "**availability**" can be understood as a promise of reliable access to certain information by authorized individuals.

forms of electronic and non-electronic information, including both commercial and personal data.

(d) ***Importance of reasonable information security.*** The need for reasonable information security measures in international arbitrations is highlighted by: the litigious backdrop of arbitration, which can lead to the targeting of information; the often high value, high stakes nature of disputes, which increases the risk of security incidents[7] and the likelihood that those incidents will cause significant loss; the exchange of information that is often confidential commercial information and/or regulated personal or other data; and the cross-border nature of the process, which creates complex challenges in complying with applicable legal requirements and heightens the consequences of a security incident.

Specific consequences that may result from inadequate attention to information security include:

– economic loss to individuals whose commercial information or personal data[8] is compromised;

---

7. The term "**security incident**" is used broadly in this Protocol to refer to an event that may have compromised the confidentiality, integrity, or availability of data or systems, such as a malware infection, loss or theft of equipment, denial of service attack, or a phishing attempt. A security incident is to be distinguished from a "**security breach**," which is a security incident that results in unauthorized access to data and/or requires that notice be given to persons whose data has been compromised and/or to supervisory authorities. Terminology used to capture these general concepts, as well as the specific definitions of the same or similar terminology, may vary by jurisdiction and under applicable laws and regulations. Thus whether a particular security incident constitutes a security breach will depend on applicable law. For example, "**data breach**" is a term of art in the GDPR, which is defined as a "breach of security leading to the accidental or unlawful destruction, loss, alternation, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed" (GDPR Art. 4(2)). Under the GDPR, there are three types of data breaches – confidentiality breach, integrity breach, or availability breach. Not all data breaches must be reported under the GDPR, although a record must be kept and the burden to establish the absence of risk that would excuse reporting rests on the data controller.
8. "**Personal data**" is a broad concept used in many of the data protection legal regimes in place around the globe, which are maturing and becoming more robust, including with respect to information security requirements. Typically, personal data is defined to include information of any nature whatsoever that, standing alone or as linked to other information, could be used to identify an individual (including, for example, work-related e-mails, lab notebooks, agreements, handwritten notes, etc.), and the term "data subject" refers to the individual to whom the personal data relates, but the exact definition and scope of personal data may vary from jurisdiction to jurisdiction. Another common term for such information is "**personally identifiable information**" ("**PII**").

- loss of integrity of data, or questions about the reliability and accuracy of data, due to a cybersecurity incident;

- unavailability of data, networks, platforms, or websites due to disruption caused by a cybersecurity incident;

- potential liability under applicable law and other regulatory frameworks, including applicable data protection regimes; and

- reputational damage to parties, arbitrators, administering institutions, and third-parties, as well as to the system of arbitration overall.

In the increasingly digital landscape in which proceedings take place, the credibility of any dispute resolution system, including arbitration, depends on maintaining a reasonable degree of protection of the information exchanged during the process, not only with respect to the information's confidentiality (except where the parties intend for the information to become public), but also its integrity and availability.

Further, arbitration has the benefit over other dispute resolution processes of enabling parties to maintain the confidentiality of the dispute resolution process itself, where they want to and where applicable law permits, and the information exchanged within it. Reasonable information security measures are essential to ensure that international arbitration maintains this advantage.

**2** **As a threshold matter, each party, arbitrator, and administering institution should consider the baseline information security practices that are addressed in Schedule A and the impact of their own information security practices on the arbitration. Effective information security in a particular arbitration requires all custodians of arbitration-related information to adopt reasonable information security practices.**

***Commentary to Principle 2***

(a) ***Baseline security.*** Principle 2 recognizes it is important that all persons who have access to arbitration-related information apply reasonable information security measures in their general business activities ("**baseline security**").

International arbitrations tend to involve a constant exchange and hosting of information among parties, tribunals, and administering institutions, which means that

they are largely digitally interdependent and any break in the security of arbitral information by any one participant in the arbitration has the potential to affect all participants and to compromise the security of the entire arbitration. Thus, the security of information in an arbitral proceeding ultimately depends on the decisions and actions of all individuals involved. Actions by any individual can be the cause of an information security incident or be the "weakest link," no matter the setting in which they practice or the infrastructure available to them. Indeed, many security incidents result from individual conduct rather than a breach of systems or infrastructure.

Because day-to-day security practices and infrastructure pre-date individual arbitration matters, pre-existing information security practices of parties, arbitrators, or administering institutions may have a significant impact on the security of the arbitration process and arbitration-related information. Thus, the participants in an arbitration may need to seek guidance from their own information technology personnel or consultants, when such resources are available.

While the need and ability to implement information security measures in a particular arbitration inevitably will vary based on the size, sophistication, and available resources of the parties, arbitrators, and any administering institution, Schedule A highlights general, readily accessible cybersecurity measures that all custodians of arbitration-related information should consider employing in their day-to-day use of technology, so as to protect the confidentiality, integrity, and availability of data in their arbitration-related activities.

Since many of the measures that are reasonable to adopt as a matter of such baseline security may also be required of the participants in an individual arbitration matter, there is significant overlap between Schedule A, which addresses baseline security measures, and Schedule C, which focuses on security measures that may be applied in individual arbitrations.

(b) ***Familiarity with existing security practices.*** Principle 2 also recognizes that familiarity with, and consideration of the adequacy of, existing information security practices and infrastructure of parties, arbitrators, and administering institutions is an essential first step in determining what information security measures should be adopted in a particular arbitration matter. Moreover, parties, arbitrators, and administering institutions may be required by law or internal practices to have procedures in place to recognize a security incident quickly.

For example, some parties, arbitrators, or administering institutions may be bound by internal policies that also will be relevant to the consideration of measures in

the arbitration, potentially including policies limiting communication with personal e-mail addresses or prohibiting the use of unencrypted portable drives (i.e., media, such as USB drives, DVDs, or hard disks, that are accessible without any further steps, such as entering passwords, to decipher their content). Individuals involved in international arbitrations should ensure that they are aware of any such policies that apply to them and that they are in compliance.

## 3 Parties, arbitrators, and administering institutions should ensure that all persons directly or indirectly involved in an arbitration on their behalf are aware of, and follow, any information security measures adopted in a proceeding, as well as the potential impact of any security incidents.

***Commentary to Principle 3***

(a) ***Information-sharing.*** Principle 3 recognizes that many persons, other than the parties, tribunals, and institutions directly involved in an arbitration, may have access to arbitration-related information and that the security of such information may be undermined if reasonable information security measures are not applied by all such persons, each of whom could cause a security incident.

(b) ***Applicable legal or other requirements.*** In some cases, legal, contractual, or ethical obligations may require that parties, arbitrators, and institutions ensure that reasonable information security measures are in place before they share arbitration-related information with others, and/or that such measures are subsequently complied with. This is often the case, for example, when a data protection law applies.

(c) ***Supporting personnel.*** Parties, arbitrators, and administering institutions may be supported by, among others, employees, lawyers, legal assistants, law clerks, trainees, administrative or other support staff, case management personnel, and tribunal secretaries. To mitigate the risk of security incidents, information security awareness should permeate organizational structures and extend to such persons, who should be made aware of, and comply with, any information security measures adopted in the arbitration.

(d) ***Independent contractors and vendors.*** Parties may engage independent contractors or third party vendors to assist with an arbitration, including, among others, consultants, experts, translators, interpreters, transcription services, document production or "e-discovery" vendors and professionals, and providers of on-line case management platforms and hearing platforms. These persons will typically

have a contractual relationship with, or be under the practical control of, a party, but will not be under the actual control of the arbitral tribunal and may not suffer directly from the consequences of an information security incident.

Parties who provide access to arbitral information covered by information security measures to such third parties should ensure that those third parties are aware of applicable security measures, have the necessary technical capabilities to comply with them, and agree to follow them. In relationships governed by contract, it will often be appropriate to expressly address information security in the agreement.

(e) ***Fact witnesses.*** Fact witnesses may need to be supplied with information related to the arbitration, yet may not be employed by, or have a contractual relationship with, any party. Where a fact witness is unable or unwilling to comply with applicable information security standards, the matter should be referred to the arbitral tribunal for consideration and, if necessary, direction.

## 4 The Protocol does not supersede applicable law, arbitration rules, professional or ethical obligations, or other binding obligations.

### *Commentary to Principle 4*

(a) ***Superseding obligations.*** Principle 4 recognizes that the Principles and other guidance in the Protocol may be subject to overriding legal or other binding obligations and that such obligations may determine or affect the information security measures that are adopted in the individual circumstances of the arbitration.

(b) ***Legal obligations, including data protection law and regulation.*** Legal requirements may apply to all individuals or entities that either process or control arbitration-related information. Furthermore, parties, arbitrators, and administering institutions may have individual responsibility for compliance with such obligations.

The most prevalent legally imposed information security requirements are those contained in many of the more than 100 national data protection laws, regulations, and industry norms applicable across the globe to certain types of personal data and data of public importance, including, for example, the GDPR in Europe, the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**") and California Consumer Privacy Act in the United States, the General Data Protection Law in Brazil, and the Personal Information Protection and Electronic Documents Act ("**PIPEDA**") in Canada.

Data protection regimes may vary from jurisdiction to jurisdiction, including with respect to what constitutes "personal data." Non-compliance with applicable law may result in substantial penalties and/or litigation risk. Furthermore, data protection enforcement and other legal risk may be inconsistent among different jurisdictions and create obstacles to transborder information exchanges, including during international arbitration proceedings. These rules are maturing and becoming more robust. It is therefore important in each case for all parties, arbitrators, and administering institutions to understand their legal obligations with respect to the processing of information, including personal data, during an arbitration.

However, although data protection laws may vary in their specific requirements, almost all require the implementation of reasonable data security measures to protect the processing of personal data. Among other things, it is important to look to applicable law to determine how applicable concepts of "reasonableness," "adequacy," "appropriateness," and "proportionality" have been applied to the required security measure, as the interpretation of these terms may differ under various legal regimes.

Where participants in the arbitration are faced with differing or conflicting legal obligations, the tribunal may need to determine, in consultation with the parties and any administering institution, how to harmonize such obligations, taking into consideration the impact on the individuals whose data is being processed, the consequences of non-compliance, principles of proportionality and due process, as well as the tribunal's role in the administration of justice. Further reference may be made to the Roadmap for a consideration of how data protection may impact the arbitration.

(c) ***Arbitration rules and institutional involvement.*** If an arbitration is administered by an institution, it may be necessary for the parties, their representatives, and the arbitral tribunal to consult and coordinate with that institution prior to adopting information security measures in order to ensure that proposed measures are consistent with, and can be implemented pursuant to, the institution's rules, practices, technical capabilities, and legal obligations. In some cases, the legal obligations of an administering institution (for example, under data protection law) may impact what information security measures are adopted by the parties and tribunal.

Depending on the sensitivity of the information involved in a particular arbitration or the nature of applicable legal obligations, coordination with the institution may be necessary at the time the arbitration is commenced or in some cases even before. This may be necessary, for example, to determine whether secure notification of a request for arbitration or request for emergency relief is possible or

whether a more limited filing may be appropriate in the first instance; to determine whether data can be transferred; or to request institutional attention to the secure handling of confidential information by potential arbitrators.

As information security receives increasing attention, some institutions are adopting their own rules and practices relating to information security. For example, institutions have started to refer expressly to information security in their rules and practice notes. Some institutions are also adopting or endorsing secure platforms for the transmission and hosting of some of the information related to arbitrations they administer. Such rules and practices may or may not be considered mandatory by the institution.

(d) ***Ethical and professional obligations.*** Ethical and professional rules and guidance increasingly address information security, often in terms of well-established duties of confidentiality and competence. Parties and tribunals should consider potentially applicable obligations of this nature. In the case of the tribunal, for example, this may include consideration of an ethical obligation to preserve and protect the legitimacy and integrity of the arbitration process.

## The Standard

**5** **Subject to Principle 4, the information security measures adopted for the arbitration shall be those that are reasonable in the circumstances of the case as considered in Principles 6–8.**

***Commentary to Principle 5***

(a) Principle 5 recognizes that there is no one-size-fits-all approach to information security in arbitration matters and that the application of the reasonableness standard in the Protocol is always subject to superseding legal and other obligations, as set forth in Principle 4.

This individualized approach recognizes that the implementation of information security measures entails balancing potentially competing considerations (such as cost and convenience) and that, subject to Principle 4, similarly situated parties may make different, but equally legitimate, choices based on their own preferences, including considerations of cost and proportionality, risk tolerance, and technical capabilities, among others.

Principles 6–8 and the related schedules provide three-step guidance on how to apply the reasonableness standard in each case. First, Principle 6 and Schedule B walk through risk factors bearing on what security measures are reasonable in particular arbitration matters. Next, Principle 7 identifies categories of information security measures that should be considered in each matter. Principle 8 then flags aspects of the arbitration process to which information security measures may be applied. Schedule C supplements Principles 7 and 8 with examples of specific information security measures and processes that might be adopted for particular arbitration matters. It is anticipated that Schedule C will require updates over time. The reasonableness standard also provides flexibility to accommodate changes in technology and the best practices and threats current at the time of an actual dispute.

## Determining Reasonable Cybersecurity Measures

**6**

**In determining which specific information security measures are reasonable for a particular arbitration, the parties and the tribunal should consider:**

**(a) the risk profile of the arbitration, taking into account the factors set forth in Schedule B;**

**(b) the existing information security practices, infrastructure, and capabilities of the parties, arbitrators, and any administering institution, and the extent to which those practices address the categories of information security measures referenced in Principle 7;**

**(c) the burden, costs, and the relative resources of the parties, arbitrators, and any administering institution;**

**(d) proportionality relative to the size, value, and risk profile of the dispute, and where data protection laws and regulations apply, to the impact on the data subject; and**

**(e) the efficiency of the arbitral process.**

### *Commentary to Principle 6*

(a) ***Factors bearing on reasonableness.*** Principle 6 sets out factors to be considered in determining what information security measures are reasonable in particular arbitration matters.

(b) ***Risk analysis.*** Principle 6(a) recommends a risk analysis to determine the risk-profile of the arbitration. Schedule B identifies relevant risk factors relating to the nature of the information expected to be shared in the arbitration, potential security threats, and the potential consequences of an information security breach.

It is possible that some aspects of an arbitration may have a higher risk profile than others, in which case the risk analysis will be useful in identifying those aspects of the case that may warrant the application of more secure measures.

(c) ***Practical considerations.*** The remainder of Principle 6 identifies practical considerations that may bear on what information security measures are reasonable. For example:

i. Consistent with Principle 2, Principle 6(b) flags that the day-to-day security practices and digital infrastructure of the parties, tribunal, and administering institution may affect what security measures are reasonable in any given arbitration matter.

For instance, if all participants already employ a level of information security appropriate to the case, additional measures may not be needed. To make such a determination, it may be appropriate in some instances for the parties, arbitrators, and any administering institution to discuss their existing information security with others, including the baseline security measures identified in Schedule A, and to agree that certain measures will be maintained during the arbitration, subject to modification under Principle 2.

ii. Principles 6(c) and (d) draw attention to the possibility that the parties, arbitrators, and any institution may have differing technical or financial resources or other constraints on their technical capacity that will influence what may be reasonable in a particular case. In such instances, it will be important to balance such limitations with all other relevant factors. Special consideration should be given to what measures may be taken without significant expenditure or resources.

iii. Principle 6(e) recognizes that if proposed information security measures would be so onerous as to prevent the arbitration from proceeding in an

orderly fashion, then the balance of "reasonableness" may weigh against their adoption. In particular, information security measures that are too difficult to implement risk being ignored or evaded, or may have a negative impact on the administration of the arbitration.

**7**

**In considering the specific information security measures to be applied in an arbitration, consideration should be given to the following categories:**

**(a) asset management;**

**(b) access controls;**

**(c) encryption;**

**(d) communications security;**

**(e) physical and environmental security;**

**(f) operations security; and**

**(g) security incident management, including breach notification expectations and procedures.**

***Commentary to Principle 7***

(a) ***Categories of information security measures.*** Upon determining what level of security is reasonable in consideration of the risk profile and other relevant circumstances under Principle 6, Principle 7 addresses the broad categories of security measures that should be considered. These categories may be useful to consider in an individual arbitration, taking into account, and adapting as necessary to reflect, the risk assessment that has been carried out pursuant to Principle 6.

While a brief explanation of each general category in Principle 7 is provided below, arbitrators, parties, and administering institutions should look to Schedule C for specific examples of how security measures within each category may be tailored to address risks present in different aspects of the arbitration, as set forth in Principle 8.

(b) ***Asset management.*** Information should be identified, classified, and controlled as appropriate for the arbitration.

Through the risk analysis in Principle 6, the parties and tribunal may have identified certain aspects of the arbitration, such as information containing commercial

trade secrets and personal data, that is of a higher risk profile than other aspects of the arbitration. It may be appropriate in such circumstances to categorize such information for the purpose of applying differing levels of protection or differing types of measures based on different risk profiles.

Retention and destruction policies that will apply during the arbitration and after its conclusion are another aspect of asset management.

(c) ***Access controls.*** Access to arbitration-related information, including access to any systems, services, devices, or applications that host such information, should be limited to authorized individuals.

Parties and the tribunal may wish to consider, for example, restricting access to arbitration data on a need-to-know basis. They might also consider policies that will apply in the arbitration with respect to the control of user accounts, passwords and multi-factor authentication (particularly where a shared platform is used to host arbitration-related data), or with respect to remote access protocols.

(d) ***Encryption.*** Encryption is the process of making plain text illegible without decryption tools, such as passwords or encryption keys. It is one of many security techniques from the field of cryptography, which deals more generally with the protection of information and communications from unauthorized recipients through the use of codes. Use of encryption should be considered where appropriate to protect the confidentiality, integrity, and availability of personal data, as well as, confidential or sensitive information in the arbitration.

(e) ***Communications security.*** The means used to communicate electronically and to share information digitally should be secure. Common means employed to protect communications security include exercising caution with attachments and links, use of secure share-file services in lieu of e-mail, and avoiding the use of public networks or, if necessary, mitigating the risks of use.

(f) ***Physical and environmental security.*** Physical access to information resources in the arbitration and to the hearing premises should be controlled to prevent unauthorized access, damage, or interference.

(g) ***Operations security.*** Operations security measures are largely concerned with ensuring the integrity of information processing systems that are used in the arbitration. What this means in practice depends on the circumstances, but such measures could include, for example, agreements regarding vulnerability monitoring, system auditing, and routine back-up of a shared platform.

(h) ***Information security incident management.*** Consideration should be given to the implementation of agreed incident response capabilities and to the timing and extent of an obligation to provide notification of a security incident. When a security incident occurs, mandatory reporting and/or other requirements under data protection laws may be triggered not only for the arbitral participant who experiences the incident, but also for other participants, whose obligations may differ. As a result, an essential step to effective management of a potential security incident in the context of an arbitration is defining expectations and procedures for breach notification at the outset of the arbitration. Schedule C, Section VII identifies general points to consider. Schedule D-1 contains sample language for such procedures, styled as a "personal data breach protocol" under the GDPR.

## 8

**In some cases, it may be reasonable to tailor the information security measures applied to the arbitration to the risks present in different aspects of the arbitration, which may include:**

**(a) information exchanges and transmission of arbitration-related information;**

**(b) storage of arbitration-related information;**

**(c) travel;**

**(d) hearings and conferences whether in-person or fully or partially remote; and/or**

**(e) post-arbitration retention and destruction policies.**

***Commentary to Principle 8***

(a) Principle 8 recognizes that certain information security measures, such as those enumerated in Principle 7, may be applied differently to different aspects of the arbitration. While examples of the categories that may be relevant to the different aspects of the arbitration are provided below, these are not intended to be exclusive, nor to suggest that each of the referenced categories or measures will be appropriate in any individual arbitration.

Furthermore, because specific measures that may be adopted are likely to change over time, as exemplified by changes in arbitration practice brought about by the pandemic, detailed examples of how the general information security categories in Principle 7 may be tailored to aspects of the arbitration process are contained in Schedule C, which the Working Group expects to revise over time.

(b) ***Information exchanges and transmission of arbitration-related information.*** Access controls, communications security, encryption, and operations security will be most relevant to securing information exchanges and transmission of arbitration-related information. The types of security measures to be considered may differ depending on the parties, tribunal, and institutions involved, and it may be appropriate to consider different measures for exchanges among parties and their representatives, the arbitral tribunal, and/or any administering institution. Consideration should be given to how transmissions of arbitral data will be made (e.g., e-mail; via third-party platform or virtual data room; USB drives or other portable storage devices) as well as to corresponding protective measures (e.g., only enterprise-grade e-mail services will be used; portable storage devices must be encrypted and the password for decryption must be communicated separately).

(c) ***Storage of arbitration-related information.*** Generally, measures in the categories of asset management, access controls, and encryption will be most relevant to the secure storage of arbitration-related information. Measures should be considered for storing communications, pleadings, disclosure materials, and evidence, and may include measures such as minimizing the processing of confidential commercial information, personal data, or other sensitive information in relation to the arbitration; limiting certain information to attorneys' eyes only; and agreeing to confidentiality provisions or implementing protective orders.

(d) ***Travel.*** Although tempered by the pandemic, the nature of international arbitration is such that travel is often involved. Travel-related information security concerns are addressed in Schedule A as a matter of baseline information security. Access controls, encryption, and physical security are relevant categories in considering measures to be applied when traveling with arbitration data.

(e) ***Hearings and conference, including videoconferences.*** Information security measures for hearings and conferences may include procedures for the handling of any transcripts, recordings, or videos which are made; restrictions on what technology (such as laptops, tablets and smartphones) attendees may bring to and use at hearings (whether in-person or fully or partially remote); features and settings of any videoconferencing platforms that may be used in the course of the arbitration; and establishing a protocol, including appropriate security measures, for remote testimony and hearings. Access controls and physical security will be relevant categories, among others, at these events in the arbitration.

(f) ***Post-arbitration document retention and destruction.*** As a matter of prudent asset management, issues to be considered with respect to post-arbitration document retention and destruction may include whether to require that arbitration-

related information be returned or safely disposed of, and the timing of any such requirement, with due consideration for applicable legal or ethical obligations, rules relating to the correction of awards and award recognition/enforcement proceedings, and legitimate interests in retaining information (e.g., for conflict checking or precedent purposes). Consideration may also be given to whether there should be a process for certification of compliance with respect to any such requirement.

## The Process to Establish Cybersecurity Measures

### 9 Taking into consideration the factors outlined in Principles 6–8 as appropriate, the parties should attempt in the first instance to agree on reasonable information security measures.

***Commentary to Principle 9***

(a) ***Importance of party autonomy.*** Principle 9 recognizes the important role that parties and their legal representatives play in establishing information security measures.

Party autonomy is fundamental in information security, as it is in other aspects of the arbitral process, and ordinarily parties and their legal representatives will take the lead in considering what information security measures should be employed for the arbitration, as they will have the best information about what security measures will be reasonable for their arbitration, as well as the greatest interest in ensuring compliance with those measures during the arbitration.

(b) ***Confer.*** In the first instance, legal representatives should generally confer concerning the information security measures to be implemented in an arbitration, taking into consideration the Principles in this Protocol.

Issues that legal representatives should consider discussing with their clients and opposing counsel may overlap with issues ordinarily considered in the context of disclosure and document preservation, and also with potential data protection issues.

## 10 Information security should be raised as early as practicable in the arbitration, which ordinarily will not be later than the first case management conference.

### *Commentary to Principle 10*

(a) ***Early case management topic.*** Principle 10 recognizes that information security should be raised as early as practicable in the arbitration. The expectation generally is for issues of information security to be discussed with the parties and, where necessary, with any administering institution, in preparation for, and during, the initial case management conference or procedural hearing and this is increasingly required by arbitration rules.

Schedule D provides sample procedural language that arbitral tribunals may use to raise issues of information security for consideration at the procedural conferenc. As discussed above under Principle 8, Schedule D-1 supplements Schedule D and provides sample language for a personal data breach protocol under the GDPR. Arbitral tribunals should also consult institutional rules and practices, which increasingly require or encourage cybersecurity and data protection to be raised at the initial procedural hearing or case management conference.

In some cases, the initial procedural hearing or case management conference may be too late to raise information security issues; in such a case, any party may raise information security measures for consideration by the tribunal or any administering institution at any time.

At the initial conference, the arbitral tribunal should be prepared to:[9]

i. engage the legal representatives in a discussion about reasonable information security measures (including breach notification expectations and procedures and other aspects of incident response);
ii. discuss the ability and willingness of its members to adopt specific security measures;
iii. address any disputes about reasonable information security measures;
iv. express its own interests in preserving the legitimacy and integrity of the arbitration process, taking into account the parties' concerns and preferences, the

9. Reference should be made to the Roadmap for consideration of data protection issues at the initial conference.

capabilities of any administering institution, and other factors discussed in this Protocol; and

v. address any other issues related to information security that it considers relevant to the proceeding.

Where cases are administered by an institution, that institution may raise issues of information security and breach notification expectations and procedures with the parties or tribunal at any time.

## 11 Taking into consideration Principles 4–9 as appropriate, the arbitral tribunal has the authority to determine the information security measures applicable to the arbitration.

***Commentary to Principle 11***

(a) ***Tribunal authority.*** Principle 11 recognizes that the arbitral tribunal has the authority to determine the information security applicable to the arbitration and that, ordinarily, it should defer to any agreement of the parties.

The general expectation is that the arbitral tribunal will incorporate directions concerning information security in an early procedural order. Schedule D and Schedule D-1 provide sample language that tribunals may use in procedural orders. Alternatively, the tribunal may simply approve and order an information security agreement made by the parties.

Where disputes arise about information security measures, the tribunal should resolve any such disputes, including any disputes about what measures should be adopted in the first instance and any disputes arising from either an agreement adopted by the parties or measures ordered by the tribunal. In case of post-arbitration disputes, it may be advisable to provide for a dispute resolution mechanism that will apply in the event that the arbitral tribunal is *functus officio* at the time of a dispute regarding information security measures. To that effect, see the sample language provided in Schedule D.

(b) ***Tribunal deference.*** The arbitral tribunal should ordinarily respect any agreement the parties have reached on the information security measures to be employed, subject to overriding legal or other obligations under Principle 4 and unless there are significant countervailing considerations. Conversely, the parties cannot unilaterally bind either the arbitral tribunal or any institution administering the arbitration. Therefore, to the extent an agreement concerning information security

between the parties impacts the arbitration process, it should be formalized only after consultation with the tribunal and, if necessary, any administering institution.

Circumstances in which the arbitral tribunal may be justified in departing from the parties' agreement may include, but are not limited to:

i. measures to protect third-party interests, including the interests of witnesses or others who may be involved in the arbitration as described in the commentary to Principle 3;
ii. capabilities of the arbitrators and administering institution; and
iii. the tribunal's own interest in protecting the legitimacy and integrity of the arbitral process, including the security of its own communications and deliberations.

(c) ***Arbitrator selection.*** If the subject matter of the arbitration itself involves the resolution of information security related issues, the parties may wish to: (i) engage arbitrators with sufficient knowledge of information security issues to resolve the issues without reliance on an independent expert; and/or (ii) use adversarial expert testimony to educate the arbitral tribunal similar to the treatment of other technical issues arising in arbitration.

## 12 The arbitral tribunal may modify the measures previously established for the arbitration, at the request of any party or on the tribunal's own initiative, in light of the evolving circumstances of the case.

### *Commentary to Principle 12*

(a) ***Evolving circumstances.*** Principle 12 recognizes that the procedures adopted at the outset of the arbitration may be modified as necessary throughout the course of the proceeding, including updates as to:

i. what qualifies as the nature of the information being processed;
ii. required procedures based on the specific circumstances of the case as it develops; and
iii. changed circumstances, such as changes in applicable law, risks in the proceeding, institutional rules/requirements, or technological developments.

(b) ***Consultation.*** Such modifications should be made after consultation with the parties and any administering institution.

## 13 In the event of a breach of the information security measures adopted for an arbitration proceeding or the occurrence of an information security incident, the arbitral tribunal may, in its discretion: (a) allocate related costs among the parties; and/or (b) impose sanctions on the parties.

***Commentary to Principle 13***

(a) ***Costs and sanctions.*** Principle 13 clarifies the power of the arbitral tribunal to order costs or sanctions in the event of a breach of the information security measures adopted for an arbitration proceeding or the occurrence of an information security incident.

The authority conferred on the arbitral tribunal in Principle 13 is implied in the tribunal's general powers and in institutional rules providing that the tribunal has the authority to administer the arbitration.

(b) ***Subject to applicable law.*** As noted in Principle 4, the arbitral tribunal's powers are subject to, and may be limited by, applicable law.

## 14 The Protocol does not establish any liability or any liability standard for any purpose, including, but not limited to, legal or regulatory purposes, liability in contract, professional malpractice, or negligence.

***Commentary to Principle 14***

(a) ***Not a liability standard.*** Principle 14 clarifies that the Protocol is not intended to establish any liability or any liability standard for any purpose.

As established throughout, the Protocol is intended to provide a general framework for how information security issues may be considered in an arbitration, and is subject to any overriding legal or other obligations that may exist. It would therefore be inappropriate to apply the Principles established by the Protocol to form any legal or other liability or responsibility.

(b) ***Party autonomy.*** Principle 14, however, is not intended to limit the right of the parties to make agreements that allocate liability for security incidents, nor is it intended to limit the power of the arbitral tribunal to issue directions regarding issues such as costs or sanctions as provided in Principle 13.

# SCHEDULES

**All views expressed in these Schedules are those of the Working Group and not of CPR, NYC Bar or ICCA, or their governing boards or members. These Schedules are the result of the collective efforts of the Working Group, the views expressed are not attributable to any particular Working Group member and all Working Group members served in their individual capacity.**

# Schedule A
# Baseline Security Measures

Schedule A supplements Principle 2 with a non-exhaustive checklist of general cybersecurity measures that all custodians of arbitration-related information should consider implementing in their day-to-day use of technology in arbitration-related activities, bearing in mind that:

- the schedule highlights various security considerations and it may not be necessary to adopt all of the measures to achieve a reasonable level of protection;

- practical and detailed guidance must be balanced with the reality that cybersecurity threats and mitigation strategies evolve rapidly, such that other practices may emerge and some of the security measures identified here may be superseded or become outdated over time; and

- these measures should be considered in conjunction with any systems, processes, policies, and procedures already in place and, where appropriate, in consultation with information technology and/or information security professionals, either within one's organization or externally.

This schedule is intended to offer a mixture of readily accessible and useful information that everyone involved in international arbitrations should consider, regardless of their practice setting or infrastructure, together with guidance that will be most helpful for those who work on their own or with minimal support and who largely manage their own digital architecture. Though it is beyond the scope of the Protocol to recommend specific products or vendors, links to resources that provide technology reviews and recommendations are provided in Schedule E.

Furthermore, although the guidance set forth here is informed by well-established, detailed technical standards for information security, most individual custodians of arbitration data will not have oversight or responsibility for full deployment of such standards (particularly in organizational settings) and do not require the level of detail or technical matter that is contained in those standards.

# Baseline Security Measures Checklist

*Click on any of the topics listed in the baseline security measures checklist below to jump to commentary on that issue.*

* * *

## *I. Knowledge and Education*

***Keep abreast of security threats and solutions.*** Effective security is an ongoing process that requires continuous attention to evolving risks and technology. For timely information about current security vulnerabilities and best practices, consider subscribing to one or more e-mail alerts or newsletters. Such alerts are free and readily available, for example, from the cybersecurity and data privacy practice groups of major law firms.

Cybersecurity training may be tailored to one's practice environment; for example, bar associations frequently offer training that is directed to solo practitioners and small law firms. Likewise, employee training and awareness at all levels of an organization is an important part of cybersecurity defense, to raise cyber-education across the board and to create a culture of security in one's organization.

***Consider professional obligations relating to cybersecurity.*** Increasingly, achieving basic competence in technology, including familiarity with measures to protect the confidentiality, integrity, and availability of digital information, is viewed as an element of professional competence; for example, in lawyer and arbitrator ethical codes.

Cybersecurity obligations may arise from other professional duties as well, such as from a duty of confidentiality. As a result, in many jurisdictions, significant cybersecurity guidance may be found in lawyer ethics opinions and on bar association websites. A sample of leading legal references and resources is contained in Schedule E.

***Consider industry standards and governmental regulations.*** There are various organizations in the information security field that have developed, and regularly update, comprehensive technical standards for cybersecurity practices and policies. Links to some of the best known standards internationally are provided in Schedule E, as are links to more accessible, simplified resources that are particularly helpful for smaller organizations and individual practitioners, such as the ICC Cyber Security Guide for Business.

In this context, also consider whether any specific technical standards should be adopted based on the types of disputes or information that typically arise in one's arbitration practice (e.g., personal data, aerospace and defense disputes, etc.), and governmental regulations that may apply as a result.

## *II. Asset Management*

***Know assets and infrastructure.*** An important first step to implementing appropriate security controls and safeguards is to know one's own data security infrastructure, including professional and personal networks and network appliances (e.g., routers and firewalls), computers, tablets, smartphones, other portable devices (such as USB drives), computer appliances (e.g., printers, scanners, internet protocol enabled video and security devices, fax machines), cloud services, software programs and apps, remote access tools, and back-up services.

It is important to have an understanding (if not a written inventory) of where data resides in, and flows through, one's digital infrastructure (or, as noted below, to be able to reasonably rely on one's organization to have that understanding). For example, an arbitrator who uses a personal tablet to review pleadings and case-related communications should know whether the documents will be stored locally on the tablet by default, on a server for applications that are used to review these documents, and/or on a cloud storage site. One should also bear in mind that confidential data may reside in non-digital formats, such as paper files.

In most cases, individuals who work in an organization that supplies systems and other resources, together with information systems support, may reasonably rely on those resources to maintain the requisite knowledge of infrastructure, data flows, and other aspects of security, provided that the organization has taken care to implement reasonable security measures and that the individual is aware of the organizational practices

and policies that apply to him or her and adheres to them. Such individuals will still need to consider data flow in connection with personal devices and infrastructure, such as any technology in a home office that is also used for work purposes.

Once one is cognizant of their own digital architecture and data flows, they can take steps to mitigate the risk of security incidents from basic security vulnerabilities.

***Identify sensitive data and take steps to minimize and protect it.*** Persons involved in international arbitrations maintain a wide array of data, ranging from data that is publicly available to data that is highly sensitive because of its confidential, commercial or personal nature. To minimize the risks of unauthorized users gaining access to sensitive data, as a general practice, it is a good idea not to accept or request sensitive data that is not needed for one's work and not to share data with anyone who does not similarly have a need for it. Such "data minimization" may also be required by various data privacy laws, such as the E.U.'s General Data Protection Regulation (GDPR).

Other general measures available to protect data that is deemed to warrant additional protection include, without limitation:

- redacting (or "masking") information (e.g., redacting party names and other identifying information in procedural orders that an arbitrator maintains from a closed matter for future consideration in other cases); and

- adding confidentiality designations to the names of documents or folders or confidentiality legends within documents so that: (i) users will consider transmitting such information by more secure means; (ii) unauthorized recipients will be alerted and on notice that they should delete or return the data if it is inadvertently disclosed; and/or (iii) the information can be readily and securely deleted when it is no longer needed.

***Avoid unnecessary multiple copies of documents.*** Avoid maintaining unnecessary multiple copies of digital or physical files and take steps to routinely look for and securely dispose of them. Be alert to the existence of copies that are created by popular digital mark-up tools, in email transmissions, through the unintentional storage of copies in cloud services linked to popular software services, such as iCloud, Adobe Creative Cloud, Microsoft Cloud, etc., and in "download" folders, and securely delete copies that are no longer required.

***Establish document retention and destruction practices.*** Consider implementing document retention and destruction practices to minimize holding data that is no longer required or no longer serves a business purpose, taking into account applicable legal

or ethical obligations, rules relating to the correction of awards and award recognition/enforcement proceedings, and legitimate interests in retaining information. Where documents and data from closed matters are retained for conflict checking, tax purposes, precedent purposes, or for other legitimate reasons, consider whether some or all of the data can be anonymized or redacted and whether it can or should be stored in archived form (e.g., segregated from active files on an offline, encrypted hard drive or secure cloud service).

Data that is no longer needed should be securely destroyed. Paper files should be shredded while digital devices and files should be securely wiped or deleted. Be sure to empty digital "trash" folders regularly and be aware that documents that have been "deleted" on a device still may be recoverable with forensic tools that are in widespread use. Consider using special programs that over-write deleted data to dispose of particularly sensitive data and always use such programs before disposing of a device.

***Enable remote location tracking and data wiping functions.*** Enable remote location tracking and wiping functions that are available on mobile devices, including phones, tablets, and laptops, and take special care to securely wipe data from devices that are no longer in use. Examples include the "Find My iPhone" or "Find My Mac" capability on Apple devices and the Android and Windows "Find My Device" capability. In larger organizations, systems support personnel may ensure that these functions are implemented in devices owned by the organization, whereas it may be the responsibility of individual users to adjust these settings on their authorized personal devices.

***Minimize access to sensitive data while traveling.*** The nature of international arbitration is such that significant travel is often involved. Travel creates risks for information security caused by traveling with arbitration related information, the use of non-secure networks, and other similar issues.

Some measures that one may consider to minimize travel-related risks are, among others:

- Turn off laptops and mobile devices before passing through border security and set them so that applications and documents do not automatically load when they are turned on. This may make it more difficult for data to be accessed (e.g., by activating full-disk encryption), though beware that in some countries, including the United States and Canada, border officials may have authority to search the content on electronic devices, including by compelling the holder to provide password or biometric (e.g., fingerprint or face recognition) access.

- Do not travel with devices that are not needed or consider traveling with a dedicated "clean" or "burner" device (i.e., a device that is reserved for travel

purposes that does not have e-mail or cloud applications installed on it and that stores only data that is essential for use in transit). One may then log in to e-mail and cloud content remotely over a secure network at the destination.

- Where the travel mode feature is available for a password manager, take advantage of it to temporarily disable access to sensitive passwords.

- Mark and segregate privileged and confidential files in a separate digital folder so that they can readily be identified as such. If questioned, assert applicable privilege or confidentiality protections when border authorities seek to access the data.

Schedule E contains references to further guidance regarding the protection of data at border crossings.

***Back-up data.*** Make routine secure and redundant data back-ups. Redundant data back-ups allow the recovery of information in the event data is lost or compromised due to human error, technical failure, ransomware attack, fire, or otherwise. One approach is to follow the so-called 3-2-1 rule, which means there should be three copies of the data in total, two different storage media should be used (e.g., one physical external and encrypted back-up drive could be used, together with a cloud-based back-up service), and one copy should be stored offsite (e.g., in the cloud). It is also commonly recommended that a "cold" back-up (i.e., a back-up that is kept offline and disconnected from one's network) be maintained so that if one's network is compromised, there will be an uncompromised back-up of the network data.

## *III. Access Controls*

Access controls determine who has authority to access accounts, devices, and information and what privileges they have with respect to those accounts, devices, and information. Among other things, access controls include user account management, strong and complex passwords, multi-factor authentication, and/or secure password storage.

***Consider access control policies.*** Robust access controls should be considered and implemented throughout one's digital architecture as necessary to protect information from unauthorized users. For example, it may be appropriate to establish rules, among other things, for how users in the organization are to create strong passwords, how they are to store them securely, how often they are to change them, restrictions on sharing passwords, what should be password-protected (ranging from routers and printers to mobile devices, software applications, and documents or folders), and what should additionally be subject to multi-factor authentication.

***Establish strong passwords or biometric controls.*** Access to accounts, devices, and information typically is protected by gateway security such as a password or biometric identification (e.g., fingerprints, face recognition, retinal scan).

While the trend is towards increased use of biometrics, which are convenient and considered secure, most users will have a continuing need for the foreseeable future to create passwords. Key recommendations made by the United States National Institute of Science and Technology ("NIST") include that passwords should be based on unique passphrases, at least 8 characters long, and easily remembered. A passphrase (or "memorized secret") is a sequence of words or text that is longer than a typical password (i.e., longer than 6–10 characters) and easy for the user to remember, but hard for anyone else (even someone who knows the user well) to guess. Thus, common dictionary words, popular quotes, past passwords, repetitive or sequential characters, and context-specific words (such as derivatives of the service being used) should be avoided. Mixtures of different character types can also be used in a passphrase, but are not strictly necessary.

***Consider password-change intervals.*** Arbitral participants may also consider how frequently they change passwords, including consideration of whether there are indications that any previous passwords have been compromised. For example, there are publicly available websites such as www.haveibeenpwned.com that may indicate whether any prior passwords have been compromised as the result of prior data breaches.

***Consider password managers.*** Security professionals often recommend the use of password managers, which are software applications that generate, store, and manage passwords. When a password manager is in place, the user need only create and remember one complex master password, thereby making it practicable for arbitrators, parties, and administering institutions to use stronger, unique passwords for every account/service being used and to change them from time to time. Some password managers also offer an audit feature which helps identify vulnerable passwords and/or have special travel settings that can be used to limit access to sensitive sites and passwords during border crossings and travel to vulnerable destinations. Before choosing a password manager, among other things, it is important to consider the commercial reputation of the service and how it handles data recovery.

***Use multi-factor authentication where available.*** Multi-factor authentication requires additional proof of identity beyond a password at the time of login. The control may consist of entering a special code transmitted by the provider to the user at login via text message, email, or a special dedicated device, such as an authentication token.

Given the frequency with which arbitrators and parties that are involved in international arbitrations travel, they may wish to ensure that any secondary authentication factor is

available offline or that there is a back-up offline alternative (such as a physical static security token or key that plugs into the device) to provide the authentication.

In some cases (when logging into e-mail, for example), it may also be possible to simplify the use of multi-factor authentication and avoid issues arising from lack of internet connectivity while traveling by entering the secondary authentication factor one-time and designating the device being used as a "trusted device." When this is done, the additional authentication is only required when a new or different device, such as a public computer, is being used.

Multi-factor authentication may be considered, in particular, for obtaining remote access to networks, systems, or platforms that contain confidential or sensitive information.

***Set up separate administrator and user accounts.*** An administrator account is a user account that has greater privileges than an ordinary user, such as to install new programs or hardware, change the usernames and passwords of others, access critical system files, and/or change security settings. To reduce the damage that a malicious program or attacker could do if they gain access to a system or account, it is generally advisable to use a standard user account (when logging in to one's computer, for example) for day-to-day work rather than an administrative account. A standard user account should have a different password than the administrative account.

***Periodically review user privileges.*** Organizations should review access control lists and user privileges for systems and accounts on a periodic basis (e.g., quarterly or annually, depending on the size of the organization, and otherwise in the event of personnel changes) and disable access for former employees and others who no longer require access.

## *IV. Encryption*

Encryption is a process that uses an algorithm to transform information to make it unreadable to unauthorized persons. Encrypted data appears as unreadable cipher text except when decrypted with one or more encryption "keys."

***Encrypt data in transit.*** Arbitral information should generally be protected during transmission using industry-standard encryption technology. Most e-mail and cloud services, with the notable exception of some free e-mail services, use transport layer security by default to protect all e-mail and documents while they are in transit over the internet. Note, though, that this is not full end-to-end encryption and the data is decrypted for processing at various steps in transit. Especially sensitive documents and communications should be transmitted by other means. As explained below regarding communications

security, if an unprotected Wi-Fi network is being used, measures to ensure that information will be encrypted in transit include using a reputable, commercial virtual private network and using websites that employ HTTPS security.

Third-party encryption software may be considered where it is appropriate to have end-to-end encryption of e-mail messages (i.e., to ensure that there is not only a secure connection for transmissions, but also that messages can be viewed only by the sender and the recipient).

***Consider file-level encryption.*** Where appropriate, specific documents or folders may be encrypted before being transmitted. Many popular applications such as Microsoft Office documents provide the option to add a password to a file to encrypt its contents.

***Enable full-disk encryption.*** To guard against unauthorized access of digital information due to loss or theft of a laptop or other mobile device, enable full-disk encryption to protect the entire hard drive of the device from all persons who lack proper sign-on credentials. On a laptop, the option to enable full-disk encryption is now built-in to the operating software (known as "BitLocker" on Windows systems and "FileVault" on Apple systems), but it must be enabled. Once enabled, a user will need an account password to logon to the device and the hard drive will be encrypted when the device is turned off (i.e., not when it is sleeping). Android and iOS devices also support full-disk encryption, as do many portable storage devices such as USB drives.

***Consider encrypting data in the cloud.*** It is generally appropriate to encrypt data before it is uploaded to a file-sharing or cloud storage service. Always use "business" or "professional" versions of such services and avoid free consumer versions, which tend to have less robust security. Some services make use of a "zero-knowledge" protocol, which means that two encryption keys are required to decipher encrypted data and the subscriber can maintain sole custody of one of the keys in a readable format rather than sharing it with the cloud provider. This feature provides the significant advantage that even if the service itself suffers a security breach, the user's data should remain inaccessible to the intruder.

## *V. Communications Security*

***Be skeptical of attachments and links.*** Phishing attacks are commonplace and sometimes highly sophisticated in mimicking known or authorized sources. Download programs and digital content only from known legitimate sources and do not open attachments or click on links from unknown email senders. Sometimes, a malicious e-mail or link may be identified simply by double-checking the sender's e-mail address for a discrepancy or hovering over, but not clicking on, a link to reveal an unrelated web address.

Moreover, if in doubt about the legitimacy of an email, contact the sender directly by telephone. Instead of clicking on the link in an email, enter the correct URL of the site in a browser and navigate directly to the website. Provide passwords or personal identifying information only when certain the request is from a legitimate website and exercise extreme caution if a site asks for such information to be re-entered. Seek out anti-phishing training.

***Consider secure share-file services in lieu of e-mail.*** Where appropriate, file-sharing or cloud storage services may be used as an alternative to e-mail for more secure transmissions. Cloud storage is a service that maintains data on remote servers that are accessed over the internet. Third party cloud storage can provide better security than an individual practitioner or small organization can reasonably provide on its own. The use of a reputable cloud service with appropriate security controls can thus be a convenient, secure, and appropriate way to store and share data.

Numerous bar association opinions in the United States have considered what due diligence should be undertaken to determine whether the use of a particular cloud storage technology or service provider is consistent with a lawyer's duty to maintain confidentiality (*see* Schedule E). The requirements typically include factors such as having a reasonable understanding of the provider's security system and its commitment to maintaining confidentiality, provisions for the user's access, protection and retrieval of data, notice provisions when third parties seek access to data, and regulatory, compliance and document retention obligations that may depend on the nature of the data and the location of the provider's servers.

***Avoid public networks or, if necessary, mitigate risks of use.*** Avoid unprotected use of public internet networks in hotels, airports, coffee shops, and elsewhere. Public Wi-Fi networks may provide hackers with access to unsecured devices on the same network, allow them to intercept password credentials, or to distribute malware. Instead of public networks, it may be preferable to use personal cellular hotspots or a wireless tether to establish an internet connection.

If it is deemed necessary to connect to a public network, the risks of such a connection may be mitigated by:

- where possible, checking the authenticity of the network username and any password with the network's owner to avoid connecting to an impostor network;

- limiting the length of the connection time (e.g., to the time needed to send drafted messages and to download new ones);

- using a reliable, commercial (paid) virtual private network (VPN) service, the purpose of which is to establish an encrypted connection over the internet for the secure transmission of data and to allow users to mask their identity from others on the network by identifying the user through the VPN; and/or

- when accessing confidential information, avoiding to connect to websites that fail to use enhanced HTTPS (which stands for hypertext transfer protocol secure and encrypts the transmission of data between two devices connected over the internet) security, as indicated in web addresses that begin with "https" rather than "http."

## *VI. Physical and Environmental Security*

Physical access to information resources should be controlled to prevent unauthorized access, damage, or interference. Preventing loss or theft of devices is especially important because many cases of digital intrusion begin with simple human error, such as leaving laptops behind in airport security lines or using non-secure computers or printers in airline clubs or hotel business centers, where copies may persist in the memory of the shared devices.

***Consider the risks of portable storage media.*** Consider the risks of using portable storage media, such as USB or "thumb" drives, which are small and easily misplaced. Never use a USB or other portable peripheral device unless you know its source, as such devices can be loaded with malicious software. Risks associated with these devices may be mitigated by encrypting the data and password-protecting the devices. Passwords should not accompany the drive or be transmitted in a way that is easily matched to the drive. For example, the password may be provided separately by telephone or text message.

***Lock devices.*** Turn off and lock computers (with a cable lock or in a docking station) when they are not in use or when away from them more than momentarily. Laptops and mobile devices should be configured to automatically lock screens after a certain period of inactivity (e.g., 5 or 10 minutes).

***Secure paper files.*** Take care to protect the information contained in paper copies of arbitration-related data. If possible, work in a dedicated location and restrict access to that area. Maintain files in secure locations and safeguard them against disasters such as fire and floods.

***Do not leave documents unattended.*** Whenever any confidential data is shipped, make it a practice to track packages and ensure that packages will not be left unattended upon

delivery (requiring signature, if necessary). Similarly, do not leave confidential data unattended on a printer, fax machine, or scanner.

***Guard against "visual hacking."*** Consider using privacy screens for laptops and mobile devices when accessing confidential information or accounts while in transit or in public or semi-public places. Also be mindful of what is available to others during videoconferences.

### *VII. Operations Security*

***Use professional, commercial products and tools.*** Avoid free or consumer versions of products and tools such as e-mail services, cloud share-file services, virtual private networks, and anti-virus software. Business and professional (or "enterprise") versions of the same tools frequently are available at a minimal cost and generally include more robust security protection. Implement available security features of these products and tools in consultation with their customer service representatives and/or information technology or information security personnel about appropriate security settings.

***Do not share devices and accounts.*** Avoid sharing devices or accounts (such as laptops, e-mail, and cloud storage) that contain business confidential information with family members or others not directly involved in one's business.

***Guard digital perimeters.*** Measures such as firewalls, antivirus, and anti-malware and anti-spyware software, which are widely available from numerous reputable vendors, guard digital "perimeters." These tools typically offer multiple settings so that the products can be customized for various users. For example, a solo practitioner or small business looking for anti-virus and anti-malware protection may consider a business or professional application (as opposed to a free, consumer version) that offers the ability to continuously scan the device or network rather than requiring manual initiation of the scan.

***Promptly install software updates and patches.*** It is critically important to promptly install updates and patches to operating systems and other software applications. Vendors frequently release updates and patches as an immediate response to identified security threats. Time is then of the essence to avoid the threat which the patch is intended to address. Avoid using any software that a developer has stopped supporting by releasing patches since unsupported software is an attractive target for malicious actors.

***Monitor for vulnerabilities.*** Arbitrators, parties, and administering institutions should regularly consider the scope and effectiveness of their security practices and take steps to remediate or mitigate any security weaknesses that they identify through such systematic

reviews. Among other things, for example, this may entail automated scans for updates and patches to operating systems and software; automated scans for malware; reviewing account access logs for, or receiving alerts of, unauthorized access to critical services; and/or configuring systems or services to identify weak password credentials.

### *VIII. Information Security Incident Response*

Notwithstanding the implementation of security and data protection measures, security incidents occur with some frequency. As addressed further in Schedule D-1, which is a sample personal data breach protocol, applicable law and sometimes professional or ethical obligations may impose breach response obligations, which may include notification to affected persons and/or regulatory authorities and other remediation measures. Arbitrators, parties, and administering institutions should consider having an incident response plan prepared in advance that includes specific plans and procedures for responding to a breach, and should also be aware that such plans and procedures could be required by applicable law. The planning and response will be facilitated by awareness of one's digital architecture and the location of one's data. It also is advisable to consider obtaining cybersecurity risk insurance, which may be available through bar associations or other sources.

# Schedule B
# Arbitral Information Security Risk Factors

Information security risk in an arbitration is a function of: the nature of the information being processed; the risks related to the subject matter of the arbitration and the participants in the process; other factors impacting the risk profile of the arbitration; and the foreseeable consequences of a breach.

Careful consideration of the risk profile of the arbitration will inform the determination of the reasonable measures to be applied in the arbitration pursuant to Principle 6. In some cases, the risk profile analysis may lead to classification of the arbitration data into different risk categories that may require differing measures of protection.

The following list is intended to help the parties and the tribunal assess the risk profile of the arbitration.

## *I. Nature of the Information*

As concerns the nature of information that is likely to be processed in the arbitration, the following factors, among others, may be considered:

(a) whether personal data, also referred to as personally identifying information ("PII"), will be processed;

(b) whether sensitive data that is legally regulated or protected will be processed (for example, under data protection legal regimes, law or regulations protecting health data, banking or personal financial records, or other sensitive categories of data);

(c) whether confidential commercial information, including financial or accounting records, will be processed;

(d) whether data of standalone value such as audio-visual content, proprietary databases, or other intellectual property will be processed; and

(e) whether the data to be processed will likely include information that is subject to express confidentiality agreements or other relevant contractual obligations.

Examples of the types of data that may require special consideration include:

(a) intellectual property;

(b) trade secrets or other commercially valuable information;

(c) health or medical information, including specially protected categories such as substance abuse treatment records and HIV/AIDS status or treatment;

(d) other categories of sensitive personal information, including data concerning racial or ethnic origins, political opinions, sexuality, religious beliefs, trade union activity, and criminal records (including sealed criminal records);

(e) payment card information;

(f) non-payment card financial information;

(g) personal data, which is also referred to as personally identifying information ("PII");

(h) information subject to a professional legal privilege, such as attorney-client or doctor-patient privilege;

(i) information related to or belonging to a government or governmental body (including classified data and politically sensitive information); and

(j) information that may be detrimental or embarrassing to a natural or legal person if released.

## *II. Risks Relating to the Subject Matter of the Arbitration or the Identity of Parties, Key Witnesses, and Other Participants (Including Arbitral Institution and Experts)*

The nature of the subject matter of the arbitration or the identity of participants in the arbitration may also impact the risk profile of the arbitration. The following factors, among others, may be considered in determining the impact of these factors on information security risk:

(a) whether the matter involves a party or other participant with a history of being targeted for cyber-attacks;

(b) whether the matter involves parties or others that handle large amounts of high value confidential commercial information and/or personal data (e.g., a law firm, bank, or health care provider);

(c) whether the matter involves a public figure, high ranking official or executive, or a celebrity; and

(d) whether the matter touches upon any government, government information, or government figure.

### *III. Other Factors Impacting the Cybersecurity Risk Profile of an Arbitration*

Other factors that may influence the cybersecurity risk profile of an arbitration include:

(a) the industry/subject matter of the dispute;

(b) the size and value of the dispute;

(c) the prevalence of cyber threats, including threats that target the industry, parties, or type of data involved in the arbitration;

(d) whether the matter is likely to attract news or media attention or impacts public policy or matters of public interest;

(e) the quantity of personal, confidential or sensitive data likely to be processed in the arbitration;

(f) the security environment in which the data is stored or communicated, including network security, the security of transmission and communications in the arbitration, and the format in which the data is stored and transmitted (e.g., whether the data is encrypted, masked, or minimized);

(g) the identity of the parties, key witnesses, any administering institution, and other individuals who may have access to the data that is processed in the arbitration; and

(h) the nature and frequency of events that increase the risk of breach, including transmissions of data, email or other communications that include the data, and the level of international travel likely to be required for the arbitration.

## *IV. Consequences of a Potential Breach*

The consequences of a breach should also be considered in deciding the risk profile of an arbitration, including:

(a) risks of potential injury caused by loss of confidentiality, availability, integrity, or authenticity of the information;

(b) risks to the integrity of the arbitration process or the nature and quality of evidence in the proceeding;

(c) financial loss, loss of privacy, destruction of value from release of confidential or proprietary data, injury to reputation or privacy of natural or legal persons, and exposure of confidential, secret, or proprietary data, keeping in mind that a breach suffered by one participant may cause injury to other participants or to third parties; and

(d) in addition to considering the potential impact of a breach on the parties, arbitrators, and any administering institution, consideration should be given to the potential risks to persons outside of the arbitration process to whom personal data relates, which is a key consideration under data protection laws.

# Schedule C
# Sample Information Security Measures

Schedule C supplements Principles 7 and 8 and includes non-exhaustive examples of specific information security measures that the parties may agree to, or the tribunal may impose, for particular arbitration matters. The measures listed here may not need to be adopted in their entirety in any individual matter, as certain measures may be viewed as alternatives to each other or as part of a complementary system. Further, because information security is changing rapidly, different or new best practices may emerge and the sample measures outlined here may be superseded or become outdated over time.

Schedule C builds upon Schedule A, which addresses general security measures that may be adopted as a regular business practice. Thus, the measures suggested here for possible adoption in individual matters should be considered in conjunction with any systems, processes, policies, and procedures already in place as part of regular business operations and in consultation with any information technology or information security professionals whose organizations are involved in the dispute and may be impacted by agreed-upon procedures.

## *I. Asset Management*

(a) Limiting exchanges of, and access to, information about the dispute to individuals on a "need to know" basis.

(b) Adopting protective measures, such as redaction (also known as masking) or pseudonymization, before the exchange of information with respect to data classified within the arbitration as higher risk.

(c) Labeling confidential or sensitive data (e.g., by adding appropriate confidentiality legends by bates stamp or to a document name). Examples of such legends include categories such as "confidential," "highly sensitive," "attorneys' eyes only" and the like, as well as categories specific to the arbitration.

(d) Not sharing disclosure material with the arbitral tribunal or the administering institution, except in respect to disclosure disputes or as required for evidentiary purposes, in which case limiting the material shared to what is relevant to, and necessary for, the tribunal's resolution of the dispute.

(e) Using a secure share site or cloud platform to share information and documents related to the dispute.

(f) Restricting use of public networks to access, store, or transmit arbitration related information.

(g) Agreeing that the parties' respective networks shall be accessed on a remote basis solely through a secure VPN.

(h) Maintaining backups of arbitration material during the pendency of the matter.

(i) Limiting the amount of time that information related to the dispute will be retained after the completion of the matter, and providing for a procedure at the conclusion of the arbitration process for such information, regardless of how stored, to be returned to the originating party, or permanently destroyed and deleted, with a process for certification of compliance.

## *II. Access Controls*

(a) Restricting access to arbitration-related information on a least-privilege and need-to-know basis, or limiting certain information to attorneys' eyes only.

(b) Agreeing on how passwords to share file sites will be communicated (typically through a separate means of communication), password protecting specific documents, and/or on expiration limits for access.

(c) Using multi-factor authentication for remote access or access to networks, systems, or platforms that may contain confidential or sensitive information related to the dispute.

(d) Conducting periodic reviews of access control lists for the systems or networks where information related to the dispute will be stored and disabling access for persons who no longer have a need to know, for example, persons who leave the employ of a party.

(e) Imposing limitations on downloading and printing hard-copy documents regarding the matter.

## *III. Encryption*

(a) Requiring information at rest, i.e., stored data, to be encrypted.

(b) Requiring information at rest, i.e., stored data, to be encrypted using zero-knowledge encryption.

(c) Agreeing to encrypt information in transit.

(d) Agreeing to encrypt devices (e.g., USB drives, hard drives) on which information related to the matter is stored or exchanged.

## *IV. Communications Security*

(a) Providing for procedures concerning how communications will occur between and among the tribunal, the parties, the administering institution and other participants in order to protect the integrity of such communications, including: (i) the transmission of communications, pleadings, and evidence by the parties; (ii) communications among arbitrators; and (iii) communications between the arbitrators and any administering institutions; and (iv) remote hearings and meetings.

(b) Using business or enterprise-level email and digital communications accounts, not free consumer or personal email services, for any emails or remote meetings regarding this matter.

(c) Using business or enterprise-level document sharing systems or software, not free consumer or personal storage or sharing, for any shared documents.

(d) Restricting the use of email files or attachments to transmit confidential or sensitive information, unless such email is end-to-end encrypted and the attachments are password-protected, with passwords to be transmitted by a separate means of communication such as text message or voicemail.

(e) In the case of a shared third-party cloud platform, agreeing on who will have access to the platform, for how long, what privileges different users will have with respect to the data, requirements for user passwords, multi-factor authentication, and remote access, as well as what vulnerability monitoring will take place.

(f) Using a shipping method with signature and tracking mechanism for delivery of any packages, drives, devices, or hard copy materials related to the dispute.

(g) Limiting or excluding the use of certain types of media (e.g., prohibiting the use of portable drives to store arbitration data) or allowing only encrypted and password protected portable drives.

(h) Using secure platforms for all remote meetings or hearings and putting in place adequate protocols addressing any specific security requirements.

## *V. Physical and Environmental Security*

(a) Taking care to prevent loss or theft of devices, including portable storage devices, and having the ability to remotely "wipe" those devices if they are lost or stolen.

(b) Taking steps to secure information contained in paper copies of arbitration-related data.

(c) Considering security measures for any hearing rooms, "war rooms," and breakout rooms, which may be located in public buildings such as hotels.

(d) Using privacy screens for laptops and mobile devices when accessing arbitration-related materials while in transit or in public places.

(e) Configuring laptops and mobile devices to automatically lock the screen after a certain period of inactivity.

## *VI. Operations Security*

(a) Patching all systems or devices that house arbitration-related information promptly when patches are issued.

(b) Monitoring for system vulnerabilities and reporting any discovered vulnerabilities to the other participants in the arbitration promptly after discovery of any vulnerability in accordance with any breach protocol or security incident response plan agreed to for the arbitration, and any applicable law or regulatory regime.

## *VII. Incident Response Management (including Breach Notification)*

(a) Implementing measures to address any information security incident that may occur over the course of the arbitration, taking into account applicable data protection laws, other regulatory regimes, or professional ethical obligations, and the parties' existing infrastructure. Schedule E includes resources that may be consulted in developing an incident response plan.

(b) Defining procedures and expectations for any notice to be provided to other arbitral participants, including the definition of a breach or a security incident that would give rise to notification obligations to others involved in the arbitration, the timing of any such notice, ongoing information sharing and cooperation with other participants regarding notifications and other remedial actions

undertaken (usually triggered upon discovery of the incident), the method of providing notice, and the recipient(s) for such notice. Notably, under the GDPR, while not all data breaches will require notification to regulators or data subjects, the burden to establish the absence of risk requiring notification rests on the data controller. Reference may be made to the Roadmap for discussion of these issues, including the definition of data controllers, and to Schedule D-1 for a sample personal data breach protocol.

(c) Agreeing to reasonably cooperate regarding any investigation and/or remediation of any notifiable information security incident related to the arbitration.

(d) Agreeing to cooperate concerning public statements made about any notifiable information security incident related to the arbitration.

# Schedule D
# Sample Language Addressing Information Security[10]

## *A. Arbitration Agreement Language*

It is not generally recommended that parties provide for specific information security measures in their arbitration agreements. First, prevailing cyber risks and technology, including technical measures available to guard against those risks, may change materially by the time a dispute arises. Second, the decision to adopt particular information security measures for an arbitration should be informed by analysis of the risk profile of the dispute and any ensuing arbitration and what is reasonable given the circumstances.

This being said, parties may want to provide generally in their arbitration agreement that reasonable security measures will be employed in the conduct of the arbitration. The following language would be appropriate for inclusion in the arbitration agreement to achieve that end:

> The Parties shall take reasonable measures to protect the security of the information processed in relation to the arbitration, taking into consideration, as appropriate, the ICCA-NYC Bar-CPR Cybersecurity Protocol for International Arbitration.

## *B. Agenda of the Initial Case Management Conference or Preliminary Hearing*

If information security has not already been addressed before the preliminary hearing or case management conference, it should be placed on the agenda for the conference. Language along the following lines could be considered for the agenda:

> The Parties should be prepared to address information security, including measures to be implemented to protect data that is exchanged, stored, or communicated in the arbitration as well as incident response measures, including breach notification expectations and procedures. The Parties are invited to consider the ICCA-NYC Bar-CPR Cybersecurity Protocol for International Arbitration. The Parties shall confer in advance of the conference and advise the Tribunal of any agreement or points of disagreement with respect to what measures to address information security are reasonable for the arbitration,

10. Reference may be made to the Roadmap for sample language that may also be considered when data protection laws may be implicated.

including whether the Tribunal should order that any particular information security measures be taken to safeguard the security of arbitration-related information.

## *C. Information Security Measures*

Taking into account any agreement of the parties with respect to reasonable information security measures, and after consideration of the parties' respective positions with respect to whether additional measures are required, the tribunal may decide to address information security in a number of ways. We have suggested below some language that may be considered or adapted for a procedural order.

### *1. Parties Agree Reasonable Information Security Measures for the Arbitration*

In preparation for the case management conference, the Parties were invited to consider information security for the arbitration and potential security incidents, including whether the Tribunal should order that any particular information security measures to safeguard the security of arbitration-related information or any measures to address any security incidents that may occur during the arbitration. Having had an opportunity to fully consider the issue, the Parties have agreed to employ the additional measures to address information security set forth in the Schedule to this Order when processing arbitration-related information during this proceeding. Each Party shall also maintain information security measures that are at least as robust as those that they follow in the normal course of business at the time of this Order when conducting this arbitration.

In addition, before exchanging sensitive personal or other data (including, but not limited to, social security or national identification numbers, financial account details, and birth dates), the Parties shall reduce the amount of sensitive data that is processed to that which is necessary and shall confer regarding redacting or otherwise masking that data to protect it from unnecessary disclosure in the arbitration. The Parties shall refrain from submitting any such information to the Tribunal in unredacted form absent prior approval of the Tribunal in consideration of the Parties' legitimate interests, including the relevance of the unredacted information.

### *2. Tribunal Prescribes Reasonable Information Security Measures for the Arbitration*

In preparation for the case management conference, the Parties were invited to consider information security for the arbitration, including, in particular, whether the Tribunal should order that any particular measures be taken to address information security including any security incidents that may occur during the arbitration. Having had an opportunity to fully consider the issue, the Parties were unable to agree. Therefore, after

consideration of the Parties' respective positions with respect to what security measures are reasonable for this matter, the Tribunal orders the Parties to employ the information security measures set forth in the Schedule to this Order when processing arbitration-related information during this proceeding. Each Party shall also maintain information security measures that are at least as robust as those that they follow in the normal course of business at the time of this Order when conducting this arbitration.

*3. Parties Agree Existing Information Security Measures Are Reasonable for the Arbitration*

In preparation for the case management conference, the Parties were invited to consider information security for the arbitration, including whether the Tribunal should order that any particular information security measures be taken to safeguard the security of arbitration-related information. Having had an opportunity to fully consider the issue, the Parties agree that: (i) the security measures that they follow in the normal course of business are reasonable for the arbitration; (ii) no additional information security measures are warranted for purposes of conducting this arbitration; and (iii) they shall follow the personal data breach protocol, or other security incident response plan, set forth in the Schedule to this Order. Each Party shall maintain information security measures that are at least as robust as those in place at the time of this Order when conducting this arbitration.

In addition, before exchanging sensitive personal or other data (including, but not limited to, social security or national identification numbers, financial account details, and birth dates), the Parties shall reduce the amount of sensitive data that is exchanged to that which is necessary and shall confer regarding redacting or otherwise masking that data to protect it from unnecessary disclosure in the arbitration. The Parties shall refrain from submitting any such information to the Tribunal in unredacted form absent prior approval of the Tribunal in consideration of the Parties' legitimate interests, including the relevance of the unredacted information.

## *D. Breach Notification Expectations and Procedures*

Refer to Schedule D-1 for sample language that can be used to address breach notification expectations and procedures during an arbitration. It is drafted in light of personal data covered by the GDPR, but similar principles apply whenever a data protection law applies to those involved in an arbitration, and putting a breach notification protocol in place is important irrespective of whether a data protection law applies.

## *E. Post-Arbitration Dispute Resolution Clause*

When parties enter into information security agreements in relation to an arbitration, they should consider that the arbitral tribunal may be *functus officio* at the time that dispute

arises under the agreement. The parties therefore may consider including language in any information security agreement they may enter into addressing the resolution of any disputes related thereto after the arbitral tribunal become *functus officio:*

> Upon the Tribunal rendering a final award or otherwise being *functus officio*, any dispute relating to information security, including, without limitation, disputes relating to data breach or incident response arising out of or relating to this Agreement, including the interpretation, breach, termination, or validity thereof, shall be finally resolved by arbitration in accordance with the [select applicable rules]. The seat of the arbitration shall be [place of arbitration]. The language of the arbitration shall be [select language]. There shall be one arbitrator [selected in accordance with the applicable rules] [who shall have experience relating to cybersecurity].

# Schedule D-1
# Sample GDPR Personal Data Breach Protocol

This Schedule provides sample language for a possible "**personal data breach**" protocol based on the GDPR.

As noted in the commentary to Principle 7, in an arbitration, a security incident experienced by any arbitral participant with respect to arbitral data including personal data may create mandatory reporting and/or other obligations not only for that arbitral participant, but also for other arbitral participants, whose obligations may differ. It is therefore important that breach notification expectations and procedures be established at the outset of the proceeding in order to enable all involved to assess and comply with any of their own obligations. It is beyond the scope of this Protocol to provide sample language under multiple legal regimes. This Schedule provides sample language for a possible "personal data breach" protocol based on the GDPR because of the GDPR's wide reach and influence on other data protection regimes.

As with all "sample" or "template" language, the language provided here should be considered only as a starting point; it should be reviewed and tailored to fit the specific facts and circumstances presented by any particular arbitration. Further, it is not intended to provide detailed guidance to individual arbitral participants regarding their reporting obligations under the GDPR or any other data protection regime. Rather, it seeks to ensure that participants are made aware in a timely fashion of incidents that may trigger obligations under GDPR or similar regimes and to provide an approach for how they might address such breaches vis-à-vis each other when they impact arbitral data including personal data.

To better understand these obligations where the GDPR applies, the European Commission has recently issued helpful guidance as to when notification is required and to whom.[11] Comprehensive guidance regarding the obligations of participants under the GDPR is also available in the Roadmap. Links to these resources are provided in Schedule E. The following overview is for context only.

11. *Guidelines 01/2021 on Examples regarding Personal Data Breach Notification,* EU Working Party, Version 2.0, adopted on 14 December 2021; *Guidelines on Personal data breach notification under Regulation 2016/679*, endorsed by the EDPB, G29 WP250 rev.1, 6 February 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

The GDPR defines a "personal data breach" as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed." Personal data under the GDPR is defined as "any information relating to an identified or identifiable natural person ('data subject')" and therefore includes much of the data processed during an arbitration.

Under the GDPR, there are three types of personal data breaches:

- "**confidentiality breach**," which is an unauthorised or accidental disclosure of, or access to, personal data;

- "**integrity breach,**" which is an unauthorised or accidental alteration of personal data; and

- "**availability breach**," which is an accidental or unauthorised loss of access to, or destruction of, personal data.

Under the GDPR, "in the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority … , unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay." (GDPR Art. 33)

Further, "when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay" unless an exception applies. (GDPR Art. 34). Hence, the presumption is that a notification must be made to the supervisory authority unless the data breach is unlikely to cause harm to data subjects.

Exceptions to the obligation to notify data subjects (note the exceptions do not apply to the obligation to notify the supervisory authority) apply where: (i) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (ii) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph (i) is no longer likely to materialize; or (iii) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner. (GDPR Art. 34).

Arbitral participants should also be mindful of any applicable professional or legal confidentiality requirements when they are required to notify a personal data breach to a supervisory authority or a data subject, but the notification requirements in the GDPR remain legally binding obligations.

* * *

## Sample GDPR Personal Data Breach Protocol

***What data does this personal data breach protocol apply to?***

This personal data breach protocol applies to the [personal data] exchanged during the course of arbitration between the parties, their counsel, the tribunal or the institution **("arbitral participants")** for purposes of the arbitration **("arbitral data").**

***What is a personal data breach?***

As used in this personal data breach protocol, "personal data breach" is defined as it is in the GDPR as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed." The GDPR defines "personal data" as "any information relating to an identified or identifiable natural person ("data subject")" and therefore includes much of the data processed during the arbitration. (GDPR Art. 4).

***What notifications may be required of a personal data breach?***

The following notifications of personal data breaches may be required during the course of the arbitration:

- To the relevant supervisory authority without undue delay and, where feasible, not later than 72 hours after becoming aware of a personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.
  Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay, and, to the extent it is not possible to provide all the information at the same time, it may do so in phases without undue further delay. (GDPR Art. 33)

- Such notification is required to contain: (i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned); (ii) its likely consequences; (iii) the measures taken or proposed to address the breach, including,

where appropriate, measures to mitigate its possible adverse effects; and (iv) the details of a contact point from whom more information can be obtained.

– To the data subjects concerned without undue delay, if data breach is likely to result in a *high risk* to the rights and freedoms of natural persons, unless an exception applies.

The notification must include the information required above, except item (i).

***If a personal data breach occurs, what should be done as among the arbitral participants?***

Any arbitral participant that becomes aware of a personal data breach involving arbitral data shall:

(i) inform the other arbitral participants of the personal data breach without undue delay after becoming aware of the personal data breach, and include the following information: (i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned); (ii) likely consequences; (iii) the measures proposed to address the breach, including, where appropriate, measures to mitigate its possible adverse effects; and (iv) the details of a contact point from whom more information can be obtained;

(ii) inform the arbitral participants, and cooperate with them to the extent feasible, regarding any notification of the data breach to any supervisory authority or data subjects, or any public disclosure concerning the data breach; and

(iii) maintain records of the personal data breach, including all details about the breach, regardless of any notification obligation.

# Schedule E
# Selected References

### *Border Crossings*

Federation of Law Societies of Canada, *Crossing the Border with Electronic Devices: What Canadian Legal Professionals Should Know* (Dec. 14, 2018), https://flsc.ca/wp-content/uploads/2019/01/Crossing-the-Border-with-Electronic-Devices-What-Canadian-Legal-Profes....pdf

New York City Bar Professional Ethics Committee, *Formal Opinion 2017-5: An Attorney's Ethical Duties Regarding U.S. Border Searches of Electronic Devices Containing Clients' Confidential Information* (May 9, 2018), https://www.nycbar.org/member-and-career-services/committees/reports-listing/reports/detail/formal-opinion-2017-5-an-attorneys-ethical-duties-regarding-us-border-searches-of-electronic-devices-containing-clients-confidential-information

### *Cybersecurity Resources for Lawyers and Arbitrators*

AAA-ICDR Best Practices Guide for Maintaining Cybersecurity and Privacy, https://www.adr.org/sites/default/files/document_repository/AAA258_Best_Practices_Cybersecurity_Privacy.pdf

AAA-ICDR Cybersecurity Checklist, https://www.adr.org/sites/default/files/document_repository/AAA259_AAA_ICDR_Cybersecurity_Checklist.pdf

AAA-ICDR Virtual Hearing Guide for Arbitrators and Parties, https://go.adr.org/rs/294-SFS-516/images/AAA268_AAA%20Virtual%20Hearing%20Guide%20for%20Arbitrators%20and%20Parties.pdf

American Bar Association, *Cybersecurity Legal Task Force*, https://www.americanbar.org/groups/cybersecurity/

American Bar Association, *Legal Technology Resource Center*, https://www.americanbar.org/groups/departments_offices/legal_technology_resources/ (including links to books, articles, and ethical opinions)

American Bar Association Standing Committee on Ethics and Professional Responsibility, *Formal Opinion 498*: Virtual Practice (Mar. 10, 2021), https://www.americanbar.org/

content/dam/aba/administrative/professional_responsibility/aba-formal-opinion-498.pdf

Association of Corporate Counsel, *Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information*, https://www.acc.com/resource-library/model-information-protection-and-security-controls-outside-counsel-possessing-0

Bar Council, *IT*, https://www.barcouncilethics.co.uk/subject/it/ (United Kingdom)

Stephanie Cohen & Mark Morril, *A Call to Cyberarms: The International Arbitrator's Duty to Avoid Digital Intrusion*, 40 FORDHAM L.J. 981 (2017), https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2657&context=ilj

Council of Bars and Law Societies of Europe, *CCBE Guidance on Improving the IT Security of Lawyers Against Unlawful Surveillance*, https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_20160520_CCBE_Guidance_on_Improving_the_IT_Security_of_Lawyers_Against_Unlawful_Surveillance.pdf

CPR Annotated Model Procedural Order for Remote Video Arbitration Proceedings, https://www.cpradr.org/resource-center/protocols-guidelines/model-procedure-order-remote-video-arbitration-proceedings

ICC Commission on Arbitration and ADR, Report DRS 898, *Leveraging Technology for Fair, Effective and Efficient International Arbitration Proceedings*, https://iccwbo.org/content/uploads/sites/3/2022/02/icc-arbitration-and-adr-commission-report-on-leveraging-technology-for-fair-effective-and-efficient-international-arbitration-proceedings.pdf (2022)

International Bar Association, *Cybersecurity Guidelines* (Oct. 2018), https://www.ibanet.org/LPRU/cybersecurity-guidelines.aspx, and Appendix A thereto (listing further reading materials from international bar associations)

International Institute for Conflict Prevention & Resolution, *CPR/FTI Consulting Cybersecurity Training*, https://www.cpradr.org/neutrals/cpr-fti-cybersecurity-training

Law Society, *Cybersecurity Guidance and Advice*, https://www.lawsociety.org.uk/support-services/practice-management/cybersecurity-and-scam-prevention/cybersecurity-guidance-and-advice/ (United Kingdom)

Queensland Law Society, *Cyber Security*, https://www.qls.com.au/Knowledge_centre/Ethics/Resources/Cyber_security (Australia)

Jill Rhodes, Robert S. Litt & Paul S. Rosenzweig, The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals (3d ed. 2022)

***Data Protection Laws and Regulations***

Daniel Cooper & Christopher Kuner, *Data Protection Law and International Dispute Resolution*, 382 Recueil des Cours: Collected Courses of the Hague Academy of International Law 174 (2017)

ICCA-IBA Joint Data Protection Task Force, *Roadmap to Data Protection in International Arbitration*, https://www.arbitration-icca.org/projects/ICCA-IBA_TaskForce.html

Kathleen Paisley, *It's All About the Data: The Impact of the EU General Data Protection Regulation on International Arbitration*, 41 FORDHAM INT'L L.J. 841 (2018)

***General Guidance***

International Chamber of Commerce, *ICC Cyber Security Guide for Business*, https://iccwbo.org/publication/icc-cyber-security-guide-for-business/

International Comparative Legal Guides, *The ICLG to: Cybersecurity Laws and Regulations 2022*, https://iclg.com/practice-areas/cybersecurity-laws-and-regulations (covering multiple jurisdictions)

National Cyber Security Centre, *Cyber Essentials*, https://www.cyberessentials.ncsc.gov.uk/

U.S. Department of Commerce, *FTC Cybersecurity Guide for Small Business*, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/small-businesses

***Glossaries***

International Association of Privacy Professionals ("IAPP"), *Glossary of Privacy Terms*, https://iapp.org/resources/glossary

National Initiative for Cybersecurity Careers and Studies ("NICCS"), *Glossary*, https://niccs.us-cert.gov/about-niccs/glossary

National Institute of Standards and Technology ("NIST"), *Glossary*, https://csrc.nist.gov/Glossary

SANS Institute, *Glossary of Security Terms*, https://www.sans.org/security-resources/glossary-of-terms

***Incident Response/Data Breach***

American Bar Association Standing Committee on Ethics and Professional Responsibility, *Formal Opinion 483: Lawyers' Obligations After an Electronic Data Breach or Cyberattack* (Oct. 17, 2018), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf

George B. Huff Jr. et al., *Best Practices for Incident Response: Achieving Preparedness Through Alignment with Voluntary Consensus Standards*, *in* ABA CYBERSECURITY HANDBOOK 289 (Jill D. Rhodes & Robert S. Litt eds., 2d ed. 2018)

*Guidelines 01/2021 on Examples regarding Personal Data Breach Notification,* EU Working Party, Version 2.0, adopted on 14 December 2021

*Guidelines on Personal data breach notification under Regulation 2016/679*, endorsed by the EDPB, G29 WP250 rev.1, 6 February 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

***Password Guidance***

NIST, *NIST Special Publication 800-63B: Digital Identity Guidelines* (June 2017 with updates as of Mar. 2, 2020), https://pages.nist.gov/800-63-3/sp800-63b.html

***Technology Reviews and Recommendations***

CNET, https://www.cnet.com/

MACWORLD, https://www.macworld.com/

Sharon D. Nelson et al., THE 2019 SOLO AND SMALL FIRM LEGAL TECHNOLOGY GUIDE (2020)

PCMAG, https://www.pcmag.com/

WIRECUTTER, https://thewirecutter.com/

### *Technical Standards*

International Organization for Standardization ("ISO"), *ISO/IEC 27000:2018 Information Technology – Security Techniques*, https://www.iso.org/standard/73906.html

NIST, *Cybersecurity Framework*, https://www.nist.gov/cyberframework

# Schedule F
# Glossary

Well-known information security glossaries are cited in Schedule E. Below is a list of terms specifically defined in the Protocol.

**Administering institution.** Administering institution, or institution, refers to any institution administering the arbitration and the individual representatives of the institution.

**Arbitral tribunal.** Arbitral tribunal, or tribunal, refers to a sole arbitrator or a panel of arbitrators.

**Availability.** Availability can be understood as a promise of reliable access to certain information by authorized individuals.

**Confidentiality.** Confidentiality can be understood as a set of rules or restrictions that limits access to certain information.

**Cybersecurity.** Cybersecurity concerns the means employed to maintain the confidentiality, integrity, and availability of digital information and is one aspect of information security.

**Data breach.** Data breach is a term of art in the GDPR defined as a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed" (GDPR Art. 4 (2)). Under the GDPR, there are three types of data breaches – confidentiality breach, integrity breach, or availability breach. Not all data breaches must be reported under GDPR, although a record must be kept and the burden to establish the absence of risk that would excuse reporting rests on the data controller.

**Information security.** Information security includes security for all types and forms of electronic and non-electronic information and includes both commercial and personal data.

**Integrity.** Integrity can be understood as an assurance that certain information is trustworthy and accurate.

**Party.** Party, or parties, refers to the parties to the arbitration and their counsel or other representatives.

**Personal data.** Personal data is a broad concept used in many of the data protection legal regimes in place around the globe, which are maturing and becoming more robust, including with respect to information security requirements. Typically, personal data is defined to include information of any nature whatsoever that standing alone or as linked to other information could be used to identify an individual (including, for example, work-related e-mails, lab notebooks, agreements, handwritten notes, etc.), but the exact definition and scope of personal data may vary from jurisdiction to jurisdiction. Another common term for such information is "**personally identifiable information**" ("**PII**").

**Processing.** Processing broadly refers to anything that is done to, or with, arbitration-related information. It includes automated and non-automated operations, such as the collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment or combination, restriction, erasure, or destruction.

**Security breach.** A security breach is a security incident that results in unauthorized access to data and/or requires that notice be given to persons whose data has been compromised and/or to supervisory authorities.

**Security incident.** Security incident broadly refers to an event that may have compromised the confidentiality, integrity, or availability of data or systems, such as a malware infection, loss or theft of equipment, denial of service attack, or a phishing attempt. Whether a particular security incident constitutes a security breach will depend on applicable law.

# Acknowledgements

The Working Group gratefully acknowledges the work of the Group's Secretaries, Eva Chan and Jesse Peters of Skadden, Arps, Slate, Meagher & Flom LLP, whose support has improved and informed our process and the quality of the Protocol. We also thank Skadden, Arps for generously making its offices available to the Working Group and for providing support throughout the process.

The ICCA representatives acknowledge with genuine thanks and appreciation the support of ICCA Presidents Lucy Reed and Gabrielle Kaufmann-Kohler (Lévy Kaufmann-Kohler), immediate past-President Donald Donovan (Debevoise & Plimpton LLP), the ICCA Governing Board, Lise Bosman (Executive Director), Lisa Bingham (Deputy Executive Director), immediate past-co-Chair Young ICCA Nhu-Hoang Tran Thang (Lalive), and the members of the ICCA Bureau, without whose support we could not have accomplished this significant and important undertaking.

The New York City Bar Association representatives extend special acknowledgement and thanks to the three interested Association committees, and their respective Chairs, who provided input throughout the process and carefully reviewed and commented on the Consultation Draft and the Protocol: the International Commercial Disputes Committee (Frances Bivens (Davis Polk & Wardwell LLP) and Richard Mattiaccio (Allegaert Berger & Vogel LLP), current and past Chairs); Arbitration (Dana MacGrath (MacGrath Arbitration) and Steve Skulnik (Thomson Reuters), past Chairs), Information Technology and Cyberlaw (Sylvia Khatcherian (Bridgewater Associates, LP), Joseph DeMarco (DeVore & DeMarco LLP) and Maia Spilman (Maia T. Spilman, LLC), past Co-Chairs). We also thank Maria Cilenti, the Association's Senior Policy Counsel, Eric Friedman, the Association's Director of Communications, and his colleague Eli Cohen for their support.

The CPR representatives thank and acknowledge the members of the CPR Cybersecurity Taskforce of the Arbitration Committee for their invaluable contribution to the Protocol. Members of the Taskforce include: Catherine Amirfar (Debevoise & Plimpton LLP); Jennifer C. Archie (Latham & Watkins LLP); Hugh Carlson (Three Crowns LLP); Mee Choi (AEGIS Insurance Services, Inc.); Javier Fernández-Samaniego (Samaniego Law); Jennifer Glasser (White & Case LLP); Benjamin Graham (Williams & Connolly LLP); Sherman Kahn (Mauriel Kapouytian Woods LLP); Bill Millar (Capgemini Services); Kenneth N. Rashbaum (Barton LLP); Hanna Roos (Hanna Roos Dispute Resolution); Jeffrey Taylor (General Motors); and Richard Ziegler (AcumenADR LLC). We also extend special thanks to the many CPR Member law firms which generously hosted cybersecurity events throughout the public consultation period.

# ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration (2022 Edition)

The ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration reviews: the importance of cybersecurity in arbitration, which has become a largely digital process; the high stakes and the risks inherent in international arbitration, including the cross-border nature of the process, which often involves extensive travel and the use of multiple networks; and factors to be considered in developing reasonable cybersecurity measures.

This 2022 edition of the Protocol was launched at the XXVth ICCA Congress held in Edinburgh, Scotland. In addition to updating the list of references found at Schedule E, the main revision from the 2020 Protocol has been to add the sample personal data breach protocol found at Schedule D-1.

These changes reflect that the cybersecurity and data protection environment in which the Protocol operates has matured in the nearly three years since the Protocol was launched, but the general principles remain the same.

The ICCA Reports No. 6

www.arbitration-icca.org