

C L I F F O R D
C H A N C E



INFORMATION SECURITY
JUNE 2023




INFORMATION SECURITY

Information is a key asset to Clifford Chance and consequently needs to be appropriately managed and protected to ensure it is not inadvertently disclosed, lost, stolen or altered. Our suppliers are expected to have effective processes and procedures in place to control and manage third party access to protected information and the premises, information technology and telecommunications systems, applications and services, and maintain confidentiality, integrity and availability of the services provided to the firm. This section outlines the minimum standards Clifford Chance expects from our third parties to support good information security management.

 <p>Compliance</p>	<p>The Supplier shall implement, maintain and abide by a written information security programme, including appropriate policies, procedures, risk assessment and other technical and organizational measures that are no less onerous than accepted industry practices (including the International Organization for Standardization's Standards: ISO/IEC 27001 – Information Security Management Systems, The National Institute of Standards and Technology (NIST) Cybersecurity Framework, or other applicable industry or national standards for information security.) These should be made available to Clifford Chance upon request. Where appropriate the Supplier shall agree to be audited on compliance with these standards.</p>
 <p>Contractual requirements</p>	<p>The Supplier shall enter into a written contract with appropriate information security obligations taking into account the requirements of applicable law and accepted industry practices to support the protection of protected information and the premises, information technology and telecommunications systems and services and ensure the continued security of information and systems in the event an agreement is terminated or transferred to another supplier.</p>
 <p>Data Storage & Transmission</p>	<p>The Supplier shall ensure that all Clifford Chance data entrusted to it is encrypted both at rest and in transit with industry standard measures. Data at rest should be encrypted with no less than 128-bit Advanced Encryption Standard (AES-128) and, as a minimum, all network transmission should be encrypted using Transport Layer Security (TLS) 1.2.</p>
 <p>Data Transfer, Deletion & Destruction</p>	<p>The Supplier shall return, delete, destroy or anonymise personal data as instructed by Clifford Chance unless it is necessary to retain the personal data for the purpose of complying with a legal obligation or to defend a legal claim.</p> <p>The Supplier shall ensure that any data returned is presented in a reasonable format that is capable of being utilised by Clifford Chance and/or a successor supplier, ensuring that a suitable process is identified to enable the migration of such data to any new system or service.</p> <p>The Supplier shall ensure that the data are not compromised during exit and that post completion of the agreed termination period the Supplier shall cease to use Clifford Chance's data. At the direction of Clifford Chance, the Supplier shall:</p> <ol style="list-style-type: none"> Provide Clifford Chance and/or a successor supplier with a complete and uncorrupted version of the data in an electronic form or such other format as specified to Clifford Chance; or Destroy, including removal of any hard disk, or return all copies of the data and confirm in writing that such destruction has taken place. Clifford Chance may request a destruction certificate from the Supplier as evidence <p>The Supplier shall erase from any computers, storage devices and storage media that are to be retained by the Supplier after the end of the agreed termination period any software containing intellectual property rights owned by Clifford Chance.</p>
 <p>Organisational and technical security</p>	<p>The Supplier shall take appropriate measures to protect Clifford Chance's information and data from accidental, unauthorised, or unlawful destruction, loss, alteration, disclosure or access.</p> <p>The Supplier will work with Clifford Chance to ensure that any data or information assets are shared securely.</p> <p>The Supplier shall take appropriate measures to secure Clifford Chance's data from unauthorised exfiltration and leakage.</p>

INFORMATION SECURITY

(CONTINUED)

 <p>Data security incidents</p>	<p>The Supplier shall notify Clifford Chance immediately, with reasonable details, if it becomes aware of, or comes to have reasonable grounds to suspect, the occurrence of any security breach or incident revealing a material weakness in the security of services provided.</p>
 <p>Employees</p>	<p>The Supplier shall be subject to appropriate Information Security approved access control measures and conduct appropriate due diligence when hiring new employees and contractors.</p> <p>All Supplier employees with access to Clifford Chance’s data should be informed of the data security requirements applicable to their role and be expected to commit to appropriate confidentiality terms.</p>
 <p>Use of Cloud / Third-Party Applications</p>	<p>The Supplier shall not place any protected information within a cloud-based or other third-party system except with Clifford Chance’s prior written approval.</p>

CLIFFORD CHANCE

Document Owner: Procurement and Information Security

Approved By: Head of Procurement and Head of Information Security

Date Approved: 19th June 2023

Date for Review: June 2024

Version: 1.0

Classification: Public

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

© Clifford Chance 2023

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

www.cliffordchance.com

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Riyadh¹ • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C. • Kyiv²

1. AS&H Clifford Chance, a joint venture entered into by Clifford Chance LLP.

2. Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.