

## **ANNEX C/ ANHANG C/ ANNEXE C/ ALLEGATO C/ ANEXO C**

### **Information Security Requirements for Suppliers**

#### **Anforderungen an die Informationssicherheit für Lieferanten**

Corden Pharma collaborates with suppliers and other business partners whose expertise and capabilities help us to support leading pharmaceutical and biotechnology companies to achieve product success for their patient's healthier lives. Suppliers and other business partners who are working on our behalf are requested to follow these Information Security Requirements for Suppliers which are aligned with the [CordenPharma Code of Conduct](#).

#### **1 Background**

The Corden Pharma Group is considered critical infrastructure by law. Disruption or impairment of Corden Pharma's ability to deliver could result in significant supply bottlenecks or risks to public safety or the affected population.

Corden Pharma takes appropriate organizational and technical precautions to prevent disruptions to ensure public supply. Corden Pharma fulfils the relevant legal and regulatory requirements, has the resulting level of security independently audited and provides evidence of this to the relevant authorities. Ensuring information security in the supply chain is one of the resulting security measures and subject to this agreement.

#### **2 Scope and General Obligations of Suppliers**

Suppliers who deliver goods and/ or services to Corden Pharma have to comply with the below IT security requirements at all times at their own cost. Supplier agrees to notify Corden Pharma of any deviations from these requirements within thirty (30) days of discovery and undertakes any and all efforts to immediately rectify the deficiencies at own cost.

Supplier ensures that these requirements are followed by its employees, as well as by the employees of any third party retained by Supplier in connection with the delivery of goods and/ or services to Corden Pharma, including subcontractors and agents.

Supplier must ensure at all times that its actions does not impair the availability, confidentiality or integrity or authenticity of the Corden Pharma's information technology systems, networks, components, data, information or processes. Supplier shall produce a valid ISO27001 certificate.

If Supplier is responsible for the provision of critical IT services, Corden Pharma may request evidence of a SOC 2 Type 2 report. Any such certification must be achieved and maintained at Supplier's cost.

The commissioning of subcontractors for IT services is only permitted with the prior naming and written consent of Corden Pharma, and Supplier shall impose on each subcontractor IT security requirements not less strict than those contained herein.

Deviations from these requirements are only permitted on a temporary basis and after written confirmation from Corden Pharma's global information security officer.

#### **3 Specific Requirements for Suppliers**

##### **3.1 Access to buildings and network**

- Insofar as Supplier employees receive access, such access shall only to be used personally by named and approved individuals within the scope of the agreed tasks or activities. The authorisation must not be transferred.

- Access may only be granted to the areas authorised by the designated contact at Corden Pharma.
- Corden Pharma reserves the right to monitor Supplier's activities on site and remotely, particularly in sensitive areas, by its own employees.
- Remote access is only permissible by means provided by Corden Pharma. Remote access may be monitored and recorded.
- Supplier must ensure that its own network does not allow uncontrolled access by third parties or supplier employees to Corden Pharma's network or systems.

### 3.2 Use of hardware, software and services provided

- Any IT devices, mobile data storage medium and means of identification (e.g. security tokens of any kind) provided by Corden Pharma:
  - must be handled properly and protected against loss or unauthorised modification;
  - Security settings may not be changed or deactivated;
  - may only be used for the fulfilment of the contract or the agreed tasks; and
  - must be returned upon termination of contract.
- Where instructed by CordenPharma personnel only hardware and software and other services approved or licensed by Corden Pharma may be used when working on Corden Pharma systems or machinery. CordenPharma reserves the right to inspect the hardware and software used on-premise.
- Industry standard workplace IT security controls must be implemented.

### 3.3 Use of own hardware and software or services

- Supplier's IT devices on which Corden pharma's data is stored or processed must be suitably secured against malware, data loss, data corruption and access by third parties. An updated and active anti-malware solution, preferably an Endpoint Detection and Response (EDR), on all general-purpose computer devices is considered the baseline. Any such system must be kept in a supported and fully patched state.
- The direct connection of the supplier's IT devices to Corden Pharma's network is prohibited unless authorized by Corden Pharma IT department.
- Mobile data storage mediums (e.g. CDs, DVDs, USB sticks, SSDs and hard drives) and mobile IT devices with information or data of the customer must be encrypted according to current German Federal Office for Information Security guidelines. The use of mobile storage shall be strictly controlled and restricted to the absolute minimum.
- Only mobile data storage media that have been checked for malware and approved by Corden Pharma's information security department may be used on Corden Pharma's devices.

### 3.4 Passwords, user IDs and user rights

- Access data and means of identification (e.g. SmartCards or security tokens, mobile phone base Multi-Factor-Authentication) may not be passed on to other persons or used to authenticate to Corden Pharma systems for other individuals than the one the credentials were issued to.
- Passwords or PINs of a user ID must be kept secret and may not be passed on or shared with other supplier employees. The password must be entered unobserved.
- Passwords, if not technically enforced, have to correspond with the specifications of Corden Pharma
- Passwords must be changed immediately if there is suspicion or certainty that unauthorised persons have gained knowledge of it.
- The user IDs and rights may only be used for the agreed upon services.

### 3.5 Handling classified information

- Supplier must comply with Corden Pharma requirements on information classification and instruct its employees on classification and associated handling requirements accordingly.
- All information and data of Corden Pharma may only be disclosed to authorised third parties after approval by the designated contact at Corden Pharma. Equivalent protection by all recipients must be ensured by Supplier.

- When transmitting Corden Pharma's information and data via public networks or storing the same on mobile data storage media, the data must be encrypted according to the guidelines of the German Federal Office for Information Security.

### 3.6 Return / disposal

- If user accounts, access rights or media for identification (e.g. security tokens, etc.) are no longer required within the term of the contract, Supplier must inform Corden Pharma immediately so that those can be blocked or deleted accordingly. This is also required if a the employment relationship with a Supplier employee with access to Corden Pharma's systems or information is terminated.
- IT devices (e.g. laptops) and mobile data storage media provided by Corden Pharma must be returned to Corden Pharma upon expiry of the contract or when they are no longer required.
- Supplier shall ensure that any loss of IT devices handed over and of media for the purpose of authentication is reported immediately to Corden Pharma by the affected Supplier's employee.
- If IT systems or components of Supplier on which data of Corden Pharma are stored are repaired or disposed of, Supplier must ensure secure deletion or destruction of all Corden Pharma data according to current guidelines of the German Federal Office for Information Security, or such other applicable law. Permanent disposal of Corden Pharma data requires prior written approval from Corden Pharma. State of the art proof of secure deletion or destruction of information/data must be provided to Corden Pharma upon request.

### 3.7 Ownership

- The sovereignty of data and the ownership of information of all kinds that are collected, created, processed or made available to Corden Pharma as described herein, and the ownership of data carriers or IT devices provided shall lie exclusively with Corden Pharma.
- Upon the expiration or termination of the underlying agreement between Supplier and Corden Pharma, all data and information must be returned to Corden Pharma and must be securely deleted from the supplier's devices and storage media. Legal requirements (e.g. statutory retention obligations) must be observed.

### 3.9 Compliance with the Law

Supplier shall comply with all applicable laws, regulations and other applicable requirements as regards to information- and cybersecurity, including but not limited to, privacy and critical infrastructure legislation, and related drug authority guidelines and requirements.

## **4 Audit Right**

Corden Pharma is entitled to audit Supplier with a prior notification of sixty (60) calendar days in order to verify the compliance with the present requirements and the implementation of the agreed measures. Corden Pharma may at its own discretion require self-assessments in-between audits. In case of a security breach, Corden Pharma is entitled to audit Supplier with a notice fourteen (14) calendar days.

## **ANHANG C**

### **Anforderungen an die Informationssicherheit für Lieferanten**

Corden Pharma arbeitet mit Lieferanten und anderen Geschäftspartnern zusammen, deren Fachwissen und Fähigkeiten uns dabei helfen, führende Pharma- und Biotechnologieunternehmen dabei zu unterstützen, mit ihren Produkten einen Beitrag zur Gesundheit ihrer Patienten zu leisten. Lieferanten und andere Geschäftspartner, die in unserem Auftrag tätig sind, sind aufgefordert, diese Anforderungen an die Informationssicherheit für Lieferanten zu befolgen, die mit dem [Verhaltenskodex von CordenPharma](#) im Einklang stehen.

#### **1 Hintergrund**

Die Corden Pharma Group gilt laut Gesetz als kritische Infrastruktur. Eine Störung oder Beeinträchtigung der Lieferfähigkeit von Corden Pharma könnte zu erheblichen Versorgungsengpässen oder Risiken für die öffentliche Sicherheit oder die betroffene Bevölkerung führen.

Corden Pharma trifft geeignete organisatorische und technische Vorkehrungen, um Störungen zu verhindern und die öffentliche Versorgung sicherzustellen. Corden Pharma erfüllt die einschlägigen gesetzlichen und behördlichen Anforderungen, lässt das daraus resultierende Sicherheitsniveau unabhängig prüfen und legt den zuständigen Behörden entsprechende Nachweise vor. Die Gewährleistung der Informationssicherheit in der Lieferkette ist eine der daraus resultierenden Sicherheitsmaßnahmen und unterliegt dieser Vereinbarung.

#### **2 Umfang und allgemeine Verpflichtungen der Lieferanten**

Lieferanten, die Waren und/oder Dienstleistungen an Corden Pharma liefern, müssen die folgenden IT-Sicherheitsanforderungen jederzeit auf eigene Kosten einhalten. Der Lieferant verpflichtet sich, Corden Pharma innerhalb von dreißig (30) Tagen nach Feststellung über Abweichungen von diesen Anforderungen zu informieren und alle Anstrengungen zu unternehmen, um die Mängel unverzüglich auf eigene Kosten zu beheben.

Der Lieferant stellt sicher, dass diese Anforderungen von seinen Mitarbeitern sowie von den Mitarbeitern aller Dritten, die der Lieferant im Zusammenhang mit der Lieferung von Waren und/oder Dienstleistungen an Corden Pharma beauftragt hat, einschließlich Subunternehmern und Vertretern, eingehalten werden.

Der Lieferant muss jederzeit sicherstellen, dass seine Handlungen die Verfügbarkeit, Vertraulichkeit, Integrität oder Authentizität der Informationstechnologiesysteme, Netzwerke, Komponenten, Daten, Informationen oder Prozesse von Corden Pharma nicht beeinträchtigen. Der Lieferant muss ein gültiges ISO27001-Zertifikat vorlegen.

Wenn der Lieferant für die Bereitstellung kritischer IT-Dienstleistungen verantwortlich ist, kann Corden Pharma einen Nachweis in Form eines SOC 2 Typ 2-Berichts verlangen. Eine solche Zertifizierung muss auf Kosten des Lieferanten erreicht und aufrechterhalten werden.

Die Beauftragung von Subunternehmern für IT-Dienstleistungen ist nur mit vorheriger namentlicher Nennung und schriftlicher Zustimmung von Corden Pharma zulässig, und der Lieferant muss jedem Subunternehmer IT-Sicherheitsanforderungen auferlegen, die nicht weniger streng sind als die hierin enthaltenen.

Abweichungen von diesen Anforderungen sind nur vorübergehend und nach schriftlicher Bestätigung durch den globalen Informationssicherheitsbeauftragten von Corden Pharma zulässig.

#### **3 Besondere Anforderungen an Lieferanten**

##### **3.1 Zugang zu Gebäuden und Netzwerk**

- Soweit Mitarbeiter des Lieferanten Zugang erhalten, darf dieser Zugang nur von namentlich genannten und zugelassenen Personen im Rahmen der vereinbarten Aufgaben oder Tätigkeiten persönlich genutzt werden. Die Berechtigung darf nicht übertragen werden.

- Der Zugang darf nur zu den Bereichen gewährt werden, die von dem benannten Ansprechpartner bei Corden Pharma genehmigt wurden.
- Corden Pharma behält sich das Recht vor, die Aktivitäten des Lieferanten vor Ort und aus der Ferne, insbesondere in sensiblen Bereichen, durch eigene Mitarbeiter zu überwachen.
- Der Fernzugang ist nur mit den von Corden Pharma bereitgestellten Mitteln zulässig. Der Fernzugang kann überwacht und aufgezeichnet werden.
- Der Lieferant muss sicherstellen, dass sein eigenes Netzwerk keinen unkontrollierten Zugriff durch Dritte oder Mitarbeiter des Lieferanten auf das Netzwerk oder die Systeme von Corden Pharma ermöglicht.

### 3.2 Nutzung der bereitgestellten Hardware, Software und Dienste

- Alle von Corden Pharma bereitgestellten IT-Geräte, mobilen Datenspeichermedien und Identifikationsmittel (z. B. Sicherheitstoken jeglicher Art)
  - müssen ordnungsgemäß behandelt und vor Verlust oder unbefugter Veränderung geschützt werden;
  - Sicherheitseinstellungen dürfen nicht geändert oder deaktiviert werden;
  - dürfen nur zur Erfüllung des Vertrags oder der vereinbarten Aufgaben verwendet werden; und
  - müssen bei Beendigung des Vertrags zurückgegeben werden.
- Auf Anweisung von CordenPharma-Mitarbeitern dürfen bei der Arbeit an Corden Pharma-Systemen oder -Maschinen nur Hardware, Software und andere Dienste verwendet werden, die von Corden Pharma genehmigt oder lizenziert sind. CordenPharma behält sich das Recht vor, die vor Ort verwendete Hardware und Software zu überprüfen.
- Es müssen branchenübliche IT-Sicherheitskontrollen am Arbeitsplatz implementiert werden.

### 3.3 Verwendung eigener Hardware und Software oder Dienste

- IT-Geräte des Lieferanten, auf denen Daten von Corden Pharma gespeichert oder verarbeitet werden, müssen angemessen gegen Malware, Datenverlust, Datenbeschädigung und Zugriff durch Dritte gesichert sein. Eine aktualisierte und aktive Anti-Malware-Lösung, vorzugsweise eine Endpoint Detection and Response (EDR), auf allen Allzweck-Computergeräten gilt als Mindestanforderung. Ein solches System muss in einem unterstützten und vollständig gepatchten Zustand gehalten werden.
- Die direkte Verbindung der IT-Geräte des Lieferanten mit dem Netzwerk von Corden Pharma ist ohne Genehmigung durch die IT-Abteilung von Corden Pharma untersagt.
- Mobile Datenträger (z. B. CDs, DVDs, USB-Sticks, SSDs und Festplatten) und mobile IT-Geräte mit Informationen oder Daten des Kunden müssen gemäß den aktuellen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik verschlüsselt werden. Die Verwendung mobiler Speichermedien ist streng zu kontrollieren und auf das absolute Minimum zu beschränken.
- Auf den Geräten von Corden Pharma dürfen nur mobile Datenträger verwendet werden, die auf Malware überprüft und von der Abteilung für Informationssicherheit von Corden Pharma genehmigt wurden.

### 3.4 Passwörter, Benutzerkennungen und Benutzerrechte

- Zugangsdaten und Identifikationsmittel (z. B. SmartCards oder Security Tokens, Multi-Faktor-Authentifizierung per Mobiltelefon) dürfen nicht an andere Personen weitergegeben oder zur Authentifizierung bei Corden Pharma-Systemen für andere Personen als diejenige verwendet werden, für die die Zugangsdaten ausgestellt wurden.
- Passwörter oder PINs einer Benutzer-ID müssen geheim gehalten werden und dürfen nicht an andere Mitarbeiter des Lieferanten weitergegeben oder mit diesen geteilt werden. Das Passwort muss unbeobachtet eingegeben werden.
- Passwörter müssen, sofern dies nicht technisch erzwungen wird, den Vorgaben von Corden Pharma entsprechen.
- Passwörter müssen sofort geändert werden, wenn der Verdacht oder die Gewissheit besteht, dass unbefugte Personen davon Kenntnis erlangt haben.
- Die Benutzerkennungen und Rechte dürfen nur für die vereinbarten Dienste verwendet werden.

### 3.5 Umgang mit vertraulichen Informationen

- Der Lieferant muss die Anforderungen von Corden Pharma zur Klassifikation von Informationen einhalten und seine Mitarbeiter entsprechend über die Einstufung und die damit verbundenen Anforderungen an den Umgang mit Informationen unterrichten.
- Alle Informationen und Daten von Corden Pharma dürfen nur nach Genehmigung durch den zuständigen Ansprechpartner bei Corden Pharma an autorisierte Dritte weitergegeben werden. Der Lieferant muss sicherstellen, dass alle Empfänger einen gleichwertigen Schutz gewährleisten.
- Bei der Übertragung von Informationen und Daten von Corden Pharma über öffentliche Netzwerke oder bei der Speicherung derselben auf mobilen Datenträgern müssen die Daten gemäß den Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik verschlüsselt werden.

### 3.6 Rückgabe/Entsorgung

- Wenn Benutzerkonten, Zugriffsrechte oder Medien zur Identifizierung (z. B. Sicherheitstoken usw.) innerhalb der Vertragslaufzeit nicht mehr benötigt werden, muss der Lieferant Corden Pharma unverzüglich informieren, damit diese entsprechend gesperrt oder gelöscht werden können. Dies ist auch erforderlich, wenn das Arbeitsverhältnis mit einem Mitarbeiter des Lieferanten, der Zugriff auf die Systeme oder Informationen von Corden Pharma hat, beendet wird.
- Von Corden Pharma zur Verfügung gestellte IT-Geräte (z. B. Laptops) und mobile Datenträger sind nach Ablauf des Vertrags oder wenn sie nicht mehr benötigt werden, an Corden Pharma zurückzugeben.
- Der Lieferant hat sicherzustellen, dass der Verlust von übergebenen IT-Geräten und Medien zur Authentifizierung unverzüglich von dem betroffenen Mitarbeiter des Lieferanten an Corden Pharma gemeldet wird.
- Werden IT-Systeme oder Komponenten des Lieferanten, auf denen Daten von Corden Pharma gespeichert sind, repariert oder entsorgt, muss der Lieferant die sichere Löschung oder Vernichtung aller Daten von Corden Pharma gemäß den aktuellen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik oder anderen geltenden Gesetzen sicherstellen. Die endgültige Entsorgung von Daten von Corden Pharma bedarf der vorherigen schriftlichen Zustimmung von Corden Pharma. Auf Anfrage muss Corden Pharma ein dem Stand der Technik entsprechender Nachweis über die sichere Löschung oder Vernichtung von Informationen/Daten vorgelegt werden.

### 3.7 Eigentumsrechte

- Die Souveränität über Daten und das Eigentum an Informationen aller Art, die wie hier beschrieben gesammelt, erstellt, verarbeitet oder Corden Pharma zur Verfügung gestellt werden, sowie das Eigentum an bereitgestellten Datenträgern oder IT-Geräten liegen ausschließlich bei Corden Pharma.
- Nach Ablauf oder Beendigung der zugrunde liegenden Vereinbarung zwischen dem Lieferanten und Corden Pharma müssen alle Daten und Informationen an Corden Pharma zurückgegeben und von den Geräten und Speichermedien des Lieferanten sicher gelöscht werden. Gesetzliche Anforderungen (z. B. gesetzliche Aufbewahrungspflichten) sind zu beachten.

### 3.9 Einhaltung der Gesetze

Der Lieferant hat alle geltenden Gesetze, Vorschriften und sonstigen Anforderungen in Bezug auf Informations- und Cybersicherheit einzuhalten, einschließlich, aber nicht beschränkt auf Datenschutz- und Kritische-Infrastruktur-Gesetze sowie damit verbundene Richtlinien und Anforderungen der Arzneimittelbehörden.

## 4 Prüfungsrecht

Corden Pharma ist berechtigt, den Lieferanten nach einer Vorankündigung von sechzig (60) Kalendertagen zu auditieren, um die Einhaltung der vorliegenden Anforderungen und die Umsetzung der vereinbarten Maßnahmen zu überprüfen. Corden Pharma kann nach eigenem Ermessen zwischen den Audits Selbstbewertungen verlangen. Im Falle einer Sicherheitsverletzung ist Corden Pharma berechtigt, den Lieferanten mit einer Frist von vierzehn (14) Kalendertagen zu auditieren.

## **ANNEXE C**

### **Exigences en matière de sécurité de l'information pour les fournisseurs**

Corden Pharma collabore avec des fournisseurs et d'autres partenaires commerciaux dont l'expertise et les capacités nous aident à accompagner les principales entreprises pharmaceutiques et de biotechnologie pour assurer le succès de leurs produits, au service d'une vie plus saine pour leurs patients. Les fournisseurs et autres partenaires commerciaux qui travaillent pour notre compte sont tenus de respecter les présentes exigences en matière de sécurité de l'information pour les fournisseurs, qui sont conformes au [code de conduite de CordenPharma](#).

#### **1 Contexte**

Le groupe Corden Pharma est considéré comme une infrastructure critique par la loi. Toute perturbation ou altération de la capacité de Corden Pharma à livrer ses produits pourrait entraîner d'importants goulets d'étranglement dans l'approvisionnement ou des risques pour la sécurité publique ou la population touchée.

Corden Pharma prend les précautions organisationnelles et techniques appropriées pour prévenir les perturbations et garantir l'approvisionnement public. Corden Pharma se conforme aux exigences légales et réglementaires applicables, fait auditer de manière indépendante le niveau de sécurité qui en résulte et fournit la preuve de cette conformité aux autorités compétentes. L'assurance de la garantie de la sécurité de l'information dans la chaîne d'approvisionnement est l'une des mesures de sécurité qui en

#### **2 Champ d'Application et Obligations Générales des Fournisseurs**

Les fournisseurs qui livrent des biens et/ou des services à Corden Pharma doivent se conformer à tout moment et à leurs propres frais aux exigences de sécurité informatique ci-dessous. Le fournisseur s'engage à informer Corden Pharma de tout écart par rapport à ces exigences dans les trente (30) jours suivant sa découverte et à mettre tout en œuvre pour remédier immédiatement aux lacunes à ses propres frais.

Le fournisseur veille à ce que ces exigences soient respectées par ses employés, ainsi que par les employés de tout tiers engagés par le fournisseur dans le cadre de la livraison de biens et/ou de services à Corden Pharma, y compris les sous-traitants et les agents.

Le fournisseur doit s'assurer à tout moment que ses actions ne portent pas atteinte à la disponibilité, à la confidentialité, l'intégrité ou l'authenticité des systèmes de technologie de l'information, des réseaux, des composants, des données, des informations ou des processus de Corden Pharma. Le fournisseur doit fournir un certificat ISO27001 valide.

Si le fournisseur est responsable de la fourniture de services informatiques critiques, Corden Pharma peut exiger la preuve d'un rapport SOC 2 Type 2. Toute certification de ce type doit être obtenue et maintenue aux frais du Fournisseur.

Le recours à des sous-traitants pour des services informatiques n'est autorisé qu'avec l'accord préalable et écrit de Corden Pharma, et le fournisseur doit imposer à chaque sous-traitant des exigences en matière de sécurité informatique au moins aussi strictes que celles contenues dans le présent document.

Les dérogations à ces exigences ne sont autorisées qu'à titre temporaire et après confirmation écrite du responsable mondial de la sécurité de l'information de Corden Pharma.

#### **3 Exigences spécifiques pour les fournisseurs**

##### **3.1 Accès aux bâtiments et au réseau**

- Dans la mesure où les employés du fournisseur bénéficient d'un accès, celui-ci ne doit être utilisé qu'à titre personnel par les personnes désignées et approuvées dans le cadre des tâches ou activités convenues. L'autorisation ne doit pas être transférée.
- L'accès ne peut être accordé qu'aux zones autorisées par le contact désigné chez Corden Pharma.
- Corden Pharma se réserve le droit de surveiller les activités du fournisseur sur site et à distance, en particulier dans les zones sensibles, par l'intermédiaire de ses propres employés.

- L'accès à distance n'est autorisé que par les moyens fournis par Corden Pharma. L'accès à distance peut être surveillé et enregistré.
- Le fournisseur doit s'assurer que son propre réseau ne permet pas l'accès incontrôlé de tiers ou d'employés du fournisseur au réseau ou aux systèmes de Corden Pharma.

### 3.2 Utilisation du matériel, des logiciels et des services fournis

- Tous les appareils informatiques, supports de stockage de données mobiles et moyens d'identification (par exemple, jetons de sécurité de toute nature) fournis par Corden Pharma :
  - doivent être manipulés correctement et protégés contre toute perte ou modification non autorisée ;
  - Les paramètres de sécurité ne peuvent être modifiés ou désactivés ;
  - Ne peuvent être utilisés que pour l'exécution du contrat ou des tâches convenues ; et
  - Doivent être restitués à la fin du contrat.
- Sur instruction du personnel de Corden Pharma, seuls le matériel, les logiciels et les autres services approuvés ou sous licence par Corden Pharma peuvent être utilisés lors du travail sur les systèmes ou les machines de Corden Pharma. Corden Pharma se réserve le droit d'inspecter le matériel et les logiciels utilisés sur place.
- Les contrôles de sécurité informatique standard de l'industrie doivent être mis en œuvre sur le lieu de travail.

#### Utilisation de matériel et de logiciel ou de services du Fournisseur

### 3.3 Utilisation de matériel et de logiciel ou de services du Fournisseur

- Les appareils informatiques du fournisseur sur lesquels les données de Corden Pharma sont stockées ou traitées doivent être correctement protégés contre les logiciels malveillants, la perte de données, la corruption de données et l'accès par des tiers. Une solution anti-malware mise à jour et active, de préférence une solution EDR (Endpoint Detection and Response), sur tous les appareils informatiques à usage général est considérée comme la norme minimale. Tout système de ce type doit être maintenu dans un état pris en charge et entièrement mis à jour.
- La connexion directe des appareils informatiques du fournisseur au réseau de Corden Pharma est interdite, sauf autorisation du service informatique de Corden Pharma.
- Les supports de stockage de données mobiles (par exemple, CD, DVD, clés USB, SSD et disques durs) et les appareils informatiques mobiles contenant des informations ou des données du client doivent être cryptés conformément aux directives actuelles de l'**Office fédéral allemand** pour la sécurité informatique. L'utilisation de supports de stockage mobiles doit être strictement contrôlée et limitée au strict minimum.
- Seuls les supports de stockage de données mobiles qui ont été vérifiés pour détecter la présence de logiciels malveillants et approuvés par le service de sécurité informatique de Corden Pharma peuvent être utilisés sur les appareils de Corden Pharma.

### 3.4 Mots de passe, identifiants et droits d'utilisateur

- Les données d'accès et les moyens d'identification (par exemple, les cartes à puce ou les jetons de sécurité, l'authentification multifactorielle par téléphone portable) ne peuvent être transmis à d'autres personnes ou utilisés pour s'authentifier sur les systèmes de Corden Pharma pour d'autres personnes que celles auxquelles les identifiants ont été délivrés.
- Les mots de passe ou codes PIN d'un identifiant utilisateur doivent rester secrets et ne peuvent être transmis ou partagés avec d'autres employés du fournisseur. Le mot de passe doit être saisi sans être observé.
- Les mots de passe, s'ils ne sont pas imposés techniquement, doivent correspondre aux spécifications de Corden Pharma.
- Les mots de passe doivent être changés immédiatement s'il y a suspicion ou certitude que des personnes non-autorisées en ont pris connaissance.
- Les identifiants et les droits d'utilisateur ne peuvent être utilisés que pour les services convenus.

### 3.5 Traitement des informations classifiées

- Le fournisseur doit se conformer aux exigences de Corden Pharma en matière de classification des informations et former ses employés à la classification et aux exigences de traitement associées.
- Toutes les informations et données de Corden Pharma ne peuvent être divulguées à des tiers autorisés qu'après accord du contact désigné chez Corden Pharma. Le fournisseur doit garantir une protection équivalente par tous les destinataires.
- Lors de la transmission des informations et données de Corden Pharma via des réseaux publics ou de leur stockage sur des supports de stockage de données mobiles, les données doivent être cryptées conformément aux directives de l'Office fédéral allemand pour la sécurité informatique.

### 3.6 Retour / Mis au rebut

- Si les comptes d'utilisateur, les droits d'accès ou les supports d'identification (par exemple, les jetons de sécurité, etc.) ne sont plus nécessaires pendant la durée du contrat, le fournisseur doit en informer immédiatement Corden Pharma afin qu'ils puissent être bloqués ou supprimés en conséquence. Cela est également nécessaire si la relation de travail avec un employé du fournisseur ayant accès aux systèmes ou aux informations de Corden Pharma prend fin.
- Les appareils informatiques (par exemple, les ordinateurs portables) et les supports de stockage de données mobiles fournis par Corden Pharma doivent être restitués à Corden Pharma à l'expiration du contrat ou lorsqu'ils ne sont plus nécessaires.
- Le fournisseur doit veiller à ce que toute perte d'appareils informatiques remis et de supports destinés à l'authentification soit immédiatement signalée à Corden Pharma par l'employé concerné du fournisseur.
- Si les systèmes informatiques ou les composants du fournisseur sur lesquels sont stockées les données de Corden Pharma sont réparés ou éliminés, le fournisseur doit veiller à la suppression ou à la destruction sécurisée de toutes les données de Corden Pharma conformément aux directives en vigueur de l'Office fédéral allemand pour la sécurité informatique ou à toute autre loi applicable. La suppression définitive des données de Corden Pharma nécessite l'accord écrit préalable de Corden Pharma. Une preuve à la pointe de la technologie de la suppression ou de la destruction sécurisée des informations/données doit être fournie à Corden Pharma sur demande.

### 3.7 Propriété

- La souveraineté des données et la propriété des informations de toute nature qui sont collectées, créées, traitées ou mises à la disposition de Corden Pharma comme décrit dans les présentes, ainsi que la propriété des supports de données ou des dispositifs informatiques fournis, appartiennent exclusivement à Corden Pharma.
- À l'expiration ou à la résiliation du contrat sous-jacent entre le fournisseur et Corden Pharma, toutes les données et informations doivent être restituées à Corden Pharma et doivent être supprimées de manière sécurisée des appareils et supports de stockage du fournisseur. Les exigences légales (par exemple, les obligations légales de conservation) doivent être respectées.

### 3.9 Respect de la loi

Le fournisseur doit se conformer à toutes les lois, réglementations et autres exigences applicables en matière de cybersécurité et de sécurité de l'information, y compris, mais sans s'y limiter, la législation sur la protection de la vie privée et les infrastructures critiques ainsi que les lignes directrices et exigences connexes des autorités en charge des médicaments.

## 4 Droit d'audit

Corden Pharma est en droit d'auditer le fournisseur moyennant un préavis de soixante (60) jours calendaires afin de vérifier le respect des présentes exigences et la mise en œuvre des mesures convenues. Corden Pharma peut, à sa seule discrétion, exiger des auto-évaluations entre les audits. En cas de violation de la sécurité, Corden Pharma est en droit d'auditer le fournisseur moyennant un préavis de quatorze (14) jours calendaires.

## **ALLEGATO C**

### **Requisiti di sicurezza delle informazioni per i fornitori**

Corden Pharma collabora con fornitori e altri partner commerciali le cui competenze e capacità ci aiutano a supportare le principali aziende farmaceutiche e biotecnologiche nel raggiungimento del successo dei loro prodotti per una vita più sana dei loro pazienti. I fornitori e gli altri partner commerciali che lavorano per nostro conto sono tenuti a seguire i presenti Requisiti di sicurezza delle informazioni per i fornitori, che sono in linea con il [Codice di condotta di CordenPharma](#).

#### **1 Contesto**

Il Gruppo Corden Pharma è considerato un'infrastruttura critica ai sensi di legge. L'interruzione o la compromissione della capacità di fornitura di Corden Pharma potrebbe causare significative difficoltà di approvvigionamento o rischi per la sicurezza pubblica o la popolazione interessata.

Corden Pharma adotta adeguate precauzioni organizzative e tecniche per prevenire interruzioni e garantire l'approvvigionamento pubblico. Corden Pharma soddisfa i requisiti legali e normativi pertinenti, sottopone il livello di sicurezza risultante a verifiche indipendenti e ne fornisce prova alle autorità competenti. Garantire la sicurezza delle informazioni nella catena di approvvigionamento è una delle misure di sicurezza risultanti e soggetta al presente accordo.

#### **2 Ambito di applicazione e obblighi generali dei fornitori**

I fornitori che consegnano beni e/o servizi a Corden Pharma devono rispettare in ogni momento e a proprie spese i requisiti di sicurezza informatica di seguito indicati. Il fornitore si impegna a comunicare a Corden Pharma eventuali scostamenti da tali requisiti entro trenta (30) giorni dalla loro scoperta e si impegna a compiere ogni sforzo per correggere immediatamente le carenze a proprie spese.

Il fornitore garantisce che tali requisiti siano rispettati dai propri dipendenti, nonché dai dipendenti di terzi incaricati dal fornitore in relazione alla fornitura di beni e/o servizi a Corden Pharma, inclusi subappaltatori e agenti.

Il Fornitore deve garantire in ogni momento che le sue azioni non compromettano la disponibilità, la riservatezza, l'integrità o l'autenticità dei sistemi informatici, delle reti, dei componenti, dei dati, delle informazioni o dei processi di Corden Pharma. Il Fornitore dovrà presentare un certificato ISO27001 valido.

Se il Fornitore è responsabile della fornitura di servizi IT critici, Corden Pharma può richiedere la prova di un rapporto SOC 2 Tipo 2. Qualsiasi certificazione di questo tipo deve essere ottenuta e mantenuta a spese del Fornitore.

Il ricorso a subappaltatori per servizi IT è consentito solo previa nomina e consenso scritto di Corden Pharma, e il Fornitore dovrà imporre a ciascun subappaltatore requisiti di sicurezza IT non meno rigorosi di quelli contenuti nel presente documento.

Deroghe a tali requisiti sono consentite solo su base temporanea e previa conferma scritta da parte del responsabile globale della sicurezza delle informazioni di Corden Pharma.

#### **3 Requisiti specifici per i fornitori**

##### **3.1 Accesso agli edifici e alla rete**

- Nella misura in cui i dipendenti del Fornitore ricevono l'accesso, tale accesso deve essere utilizzato solo personalmente da individui nominati e approvati nell'ambito dei compiti o delle attività concordati. L'autorizzazione non può essere trasferita.
- L'accesso può essere concesso solo alle aree autorizzate dal referente designato di Corden Pharma.
- Corden Pharma si riserva il diritto di monitorare le attività del Fornitore in loco e da remoto, in particolare nelle aree sensibili, tramite i propri dipendenti.

- L'accesso remoto è consentito solo tramite i mezzi forniti da Corden Pharma. L'accesso remoto può essere monitorato e registrato.
- Il Fornitore deve garantire che la propria rete non consenta l'accesso incontrollato da parte di terzi o dei propri dipendenti alla rete o ai sistemi di Corden Pharma.

### 3.2 Utilizzo di hardware, software e servizi forniti

- Qualsiasi dispositivo IT, supporto di memorizzazione dati mobile e mezzo di identificazione (ad es. token di sicurezza di qualsiasi tipo) fornito da Corden Pharma:
  - devono essere gestiti in modo adeguato e protetti da smarrimento o modifiche non autorizzate;
  - le impostazioni di sicurezza non possono essere modificate o disattivate;
  - possono essere utilizzati solo per l'adempimento del contratto o dei compiti concordati; e
  - devono essere restituiti alla scadenza del contratto.
- Su indicazione del personale di Corden Pharma, quando si lavora sui sistemi o sui macchinari di Corden Pharma è consentito utilizzare solo hardware, software e altri servizi approvati o concessi in licenza da Corden Pharma. Corden Pharma si riserva il diritto di ispezionare l'hardware e il software utilizzati in loco.
- Devono essere implementati controlli di sicurezza IT sul posto di lavoro conformi agli standard del settore.

### 3.3 Utilizzo di hardware, software o servizi propri

- I dispositivi IT del fornitore su cui sono memorizzati o elaborati i dati di Corden Pharma devono essere adeguatamente protetti da malware, perdita di dati, danneggiamento dei dati e accesso da parte di terzi. Una soluzione anti-malware aggiornata e attiva, preferibilmente un Endpoint Detection and Response (EDR), su tutti i dispositivi informatici di uso generale è considerata la base di riferimento. Qualsiasi sistema di questo tipo deve essere mantenuto in uno stato supportato e completamente aggiornato.
- È vietato il collegamento diretto dei dispositivi IT del fornitore alla rete di Corden Pharma, salvo autorizzazione del reparto IT di Corden Pharma.
- I supporti di memorizzazione dati mobili (ad es. CD, DVD, chiavette USB, SSD e dischi rigidi) e i dispositivi IT mobili contenenti informazioni o dati del cliente devono essere crittografati secondo le attuali linee guida dell'Ufficio federale tedesco per la sicurezza informatica. L'uso di supporti di memorizzazione mobili deve essere rigorosamente controllato e limitato al minimo indispensabile.
- Sui dispositivi di Corden Pharma possono essere utilizzati solo supporti di memorizzazione dati mobili che sono stati controllati per verificare la presenza di malware e approvati dal reparto di sicurezza informatica di Corden Pharma.

### 3.4 Password, ID utente e diritti utente

- I dati di accesso e i mezzi di identificazione (ad es. SmartCard o token di sicurezza, autenticazione multifattoriale tramite cellulare) non possono essere ceduti ad altre persone né utilizzati per l'autenticazione ai sistemi di Corden Pharma da parte di persone diverse da quelle a cui sono state rilasciate le credenziali.
- Le password o i PIN di un ID utente devono essere tenuti segreti e non possono essere ceduti o condivisi con altri dipendenti del fornitore. La password deve essere inserita senza essere osservata.
- Le password, se non imposte tecnicamente, devono corrispondere alle specifiche di Corden Pharma
- Le password devono essere modificate immediatamente se si sospetta o si ha la certezza che persone non autorizzate ne siano venute a conoscenza.
- Gli ID utente e i diritti possono essere utilizzati solo per i servizi concordati.

### 3.5 Trattamento delle informazioni classificate

- Il fornitore deve rispettare i requisiti di Corden Pharma in materia di classificazione delle informazioni e istruire i propri dipendenti sulla classificazione e sui relativi requisiti di trattamento.
- Tutte le informazioni e i dati di Corden Pharma possono essere divulgati a terzi autorizzati solo previa approvazione del referente designato da Corden Pharma. Il fornitore deve garantire una protezione equivalente da parte di tutti i destinatari.

- Quando si trasmettono informazioni e dati di Corden Pharma tramite reti pubbliche o si memorizzano gli stessi su supporti di memorizzazione dati mobili, i dati devono essere crittografati secondo le linee guida dell'Ufficio federale tedesco per la sicurezza informatica.

### 3.6 Restituzione/smaltimento

- Se gli account utente, i diritti di accesso o i supporti per l'identificazione (ad es. token di sicurezza, ecc.) non sono più necessari entro la durata del contratto, il Fornitore deve informare immediatamente Corden Pharma in modo che possano essere bloccati o cancellati di conseguenza. Ciò è richiesto anche in caso di cessazione del rapporto di lavoro con un dipendente del Fornitore che ha accesso ai sistemi o alle informazioni di Corden Pharma.
- I dispositivi IT (ad es. laptop) e i supporti di memorizzazione dati mobili forniti da Corden Pharma devono essere restituiti a Corden Pharma alla scadenza del contratto o quando non sono più necessari.
- Il Fornitore deve garantire che qualsiasi smarrimento dei dispositivi IT consegnati e dei supporti utilizzati per l'autenticazione sia immediatamente segnalato a Corden Pharma dal dipendente del Fornitore interessato.
- Se i sistemi informatici o i componenti del Fornitore su cui sono memorizzati i dati di Corden Pharma vengono riparati o smaltiti, il Fornitore deve garantire la cancellazione o la distruzione sicura di tutti i dati di Corden Pharma secondo le attuali linee guida dell'Ufficio federale tedesco per la sicurezza informatica o altre leggi applicabili. Lo smaltimento definitivo dei dati di Corden Pharma richiede la previa approvazione scritta da parte di Corden Pharma. Su richiesta, deve essere fornita a Corden Pharma una prova aggiornata della cancellazione o della distruzione sicura delle informazioni/dei dati.

### 3.7 Proprietà

- La sovranità dei dati e la proprietà delle informazioni di ogni tipo raccolte, create, elaborate o messe a disposizione di Corden Pharma come descritto nel presente documento, nonché la proprietà dei supporti dati o dei dispositivi IT forniti, spettano esclusivamente a Corden Pharma.
- Alla scadenza o alla risoluzione del contratto sottostante tra il Fornitore e Corden Pharma, tutti i dati e le informazioni devono essere restituiti a Corden Pharma e devono essere cancellati in modo sicuro dai dispositivi e dai supporti di memorizzazione del fornitore. Devono essere rispettati i requisiti legali (ad esempio gli obblighi di conservazione previsti dalla legge).

### 3.9 Conformità alla legge

Il Fornitore è tenuto a rispettare tutte le leggi, i regolamenti e gli altri requisiti applicabili in materia di sicurezza informatica e delle informazioni, inclusi, a titolo esemplificativo ma non esaustivo, la legislazione sulla privacy e sulle infrastrutture critiche, nonché le linee guida e i requisiti delle autorità competenti in materia di farmaci.

## 4 Diritto di audit

Corden Pharma ha il diritto di sottoporre il Fornitore a revisione previa notifica di sessanta (60) giorni di calendario al fine di verificare la conformità ai presenti requisiti e l'attuazione delle misure concordate. Corden Pharma può, a sua discrezione, richiedere autovalutazioni tra una revisione e l'altra. In caso di violazione della sicurezza, Corden Pharma ha il diritto di sottoporre il Fornitore a revisione con un preavviso di quattordici (14) giorni di calendario.

## **ANEXO C**

### **Requisitos de segurança da informação para fornecedores**

A Corden Pharma colabora com fornecedores e outros parceiros comerciais cuja experiência e capacidades nos ajudam a apoiar empresas farmacêuticas e biotecnológicas líderes a alcançar o sucesso dos seus produtos para uma vida mais saudável dos seus pacientes. Os fornecedores e outros parceiros comerciais que trabalham em nosso nome devem seguir estes Requisitos de segurança da informação para fornecedores, que estão alinhados com o [Código de Conduta da CordenPharma](#).

#### **1 Contexto**

O Grupo Corden Pharma é considerado uma infraestrutura crítica por lei. A interrupção ou comprometimento da capacidade de entrega da Corden Pharma pode resultar em gargalos significativos no abastecimento ou riscos à segurança pública ou à população afetada.

A Corden Pharma toma as precauções organizacionais e técnicas adequadas para evitar interrupções e garantir o abastecimento público. A Corden Pharma cumpre os requisitos legais e regulamentares relevantes, submete o nível de segurança resultante a uma auditoria independente e fornece provas disso às autoridades competentes. Garantir a segurança da informação na cadeia de abastecimento é uma das medidas de segurança resultantes e está sujeita a este acordo.

#### **2 Âmbito e obrigações gerais dos fornecedores**

Os fornecedores que entregam bens e/ou prestam serviços à Corden Pharma têm de cumprir os requisitos de segurança de TI abaixo indicados em todos os momentos, a suas próprias custas. O fornecedor concorda em notificar a Corden Pharma de quaisquer desvios destes requisitos no prazo de trinta (30) dias após a sua descoberta e compromete-se a envidar todos os esforços para corrigir imediatamente as deficiências, a suas próprias custas.

O fornecedor garante que estes requisitos são cumpridos pelos seus funcionários, bem como pelos funcionários de terceiros contratados pelo fornecedor em relação ao fornecimento de bens e/ou serviços à Corden Pharma, incluindo subcontratados e agentes.

O fornecedor deve garantir, em todos os momentos, que as suas ações não prejudiquem a disponibilidade, confidencialidade, integridade ou autenticidade dos sistemas de tecnologia da informação, redes, componentes, dados, informações ou processos da Corden Pharma. O fornecedor deve apresentar um certificado ISO27001 válido.

Se o Fornecedor for responsável pela prestação de serviços críticos de TI, a Corden Pharma poderá solicitar provas de um relatório SOC 2 Tipo 2. Qualquer certificação deste tipo deve ser obtida e mantida a expensas do Fornecedor.

A contratação de subcontratados para serviços de TI só é permitida com a nomeação prévia e o consentimento por escrito da Corden Pharma, e o fornecedor deve impor a cada subcontratado requisitos de segurança de TI não menos rigorosos do que os aqui contidos.

Os desvios a estes requisitos só são permitidos a título temporário e após confirmação por escrito do responsável global pela segurança da informação da Corden Pharma.

#### **3 Requisitos específicos para fornecedores**

##### **3.1 Acesso a edifícios e rede**

- Na medida em que os funcionários do Fornecedor tenham acesso, esse acesso só deve ser utilizado pessoalmente por indivíduos nomeados e aprovados no âmbito das tarefas ou atividades acordadas. A autorização não pode ser transferida.
- O acesso só pode ser concedido às áreas autorizadas pelo contacto designado na Corden Pharma.

- A Corden Pharma reserva-se o direito de monitorizar as atividades do fornecedor no local e remotamente, particularmente em áreas sensíveis, por meio de seus próprios funcionários.
- O acesso remoto só é permitido através dos meios fornecidos pela Corden Pharma. O acesso remoto pode ser monitorizado e gravado.
- O Fornecedor deve garantir que a sua própria rede não permite o acesso não controlado por terceiros ou funcionários do fornecedor à rede ou aos sistemas da Corden Pharma.

### 3.2 Utilização de hardware, software e serviços fornecidos

- Quaisquer dispositivos de TI, meios de armazenamento de dados móveis e meios de identificação (por exemplo, tokens de segurança de qualquer tipo) fornecidos pela Corden Pharma:
  - devem ser manuseados adequadamente e protegidos contra perda ou modificação não autorizada;
  - As configurações de segurança não podem ser alteradas ou desativadas;
  - só podem ser utilizados para o cumprimento do contrato ou das tarefas acordadas; e
  - devem ser devolvidos após a rescisão do contrato.
- Quando instruído pelo pessoal da Corden Pharma, apenas hardware, software e outros serviços aprovados ou licenciados pela Corden Pharma podem ser utilizados ao trabalhar em sistemas ou máquinas da Corden Pharma. A Corden Pharma reserva-se o direito de inspecionar o hardware e software utilizados nas instalações.
- Devem ser implementados controlos de segurança de TI no local de trabalho, de acordo com os padrões da indústria.

### 3.3 Utilização de hardware, software ou serviços próprios

- Os dispositivos de TI do fornecedor nos quais os dados da Corden Pharma são armazenados ou processados devem ser adequadamente protegidos contra malware, perda de dados, corrupção de dados e acesso por terceiros. Uma solução antimalware atualizada e ativa, de preferência um Endpoint Detection and Response (EDR), em todos os dispositivos de computador de uso geral é considerada a base. Qualquer sistema desse tipo deve ser mantido em um estado suportado e totalmente atualizado.
- A ligação direta dos dispositivos de TI do fornecedor à rede da Corden Pharma é proibida, a menos que autorizada pelo departamento de TI da Corden Pharma.
- Os suportes de armazenamento de dados móveis (por exemplo, CDs, DVDs, pen drives, SSDs e discos rígidos) e os dispositivos de TI móveis com informações ou dados do cliente devem ser encriptados de acordo com as diretrizes atuais do Gabinete Federal Alemão para a Segurança da Informação. A utilização de armazenamento móvel deve ser rigorosamente controlada e restringida ao mínimo absoluto.
- Apenas meios de armazenamento de dados móveis que tenham sido verificados quanto à presença de malware e aprovados pelo departamento de segurança da informação da Corden Pharma podem ser utilizados nos dispositivos da Corden Pharma.

### 3.4 Palavras-passe, IDs de utilizador e direitos de utilizador

- Os dados de acesso e meios de identificação (por exemplo, SmartCards ou tokens de segurança, autenticação multifatorial por telemóvel) não podem ser transmitidos a outras pessoas ou utilizados para autenticação nos sistemas da Corden Pharma por outras pessoas que não aquelas a quem as credenciais foram emitidas.
- As palavras-passe ou PINs de um ID de utilizador devem ser mantidos em segredo e não podem ser transmitidos ou partilhados com outros funcionários do fornecedor. A palavra-passe deve ser introduzida sem ser observada.
- As palavras-passe, se não forem impostas tecnicamente, têm de corresponder às especificações da Corden Pharma
- As palavras-passe devem ser alteradas imediatamente se houver suspeita ou certeza de que pessoas não autorizadas tomaram conhecimento delas.
- As IDs de utilizador e os direitos só podem ser utilizados para os serviços acordados.

### 3.5 Tratamento de informações confidenciais

- O fornecedor deve cumprir os requisitos da Corden Pharma em matéria de classificação de informações e instruir os seus funcionários sobre a classificação e os requisitos de tratamento associados em conformidade.
- Todas as informações e dados da Corden Pharma só podem ser divulgados a terceiros autorizados após aprovação pelo contacto designado na Corden Pharma. O fornecedor deve garantir uma proteção equivalente por parte de todos os destinatários.
- Ao transmitir informações e dados da Corden Pharma através de redes públicas ou armazená-los em suportes de armazenamento de dados móveis, os dados devem ser encriptados de acordo com as diretrizes do Gabinete Federal Alemão para a Segurança da Informação.

### 3.6 Devolução/eliminação

- Se as contas de utilizador, direitos de acesso ou meios de identificação (por exemplo, tokens de segurança, etc.) não forem mais necessários dentro do prazo do contrato, o Fornecedor deve informar imediatamente a Corden Pharma para que possam ser bloqueados ou eliminados em conformidade. Isso também é necessário se a relação de trabalho com um funcionário do Fornecedor com acesso aos sistemas ou informações da Corden Pharma for rescindida.
- Os dispositivos de TI (por exemplo, computadores portáteis) e meios de armazenamento de dados móveis fornecidos pela Corden Pharma devem ser devolvidos à Corden Pharma após o término do contrato ou quando não forem mais necessários.
- O Fornecedor deve garantir que qualquer perda de dispositivos de TI entregues e de suportes para fins de autenticação seja imediatamente comunicada à Corden Pharma pelo funcionário do Fornecedor afetado.
- Se os sistemas ou componentes de TI do Fornecedor nos quais os dados da Corden Pharma estão armazenados forem reparados ou eliminados, o Fornecedor deve garantir a eliminação ou destruição segura de todos os dados da Corden Pharma, de acordo com as diretrizes atuais do Gabinete Federal Alemão para a Segurança da Informação ou outra legislação aplicável. A eliminação permanente dos dados da Corden Pharma requer a aprovação prévia por escrito da Corden Pharma. Deve ser fornecida à Corden Pharma, mediante solicitação, prova da eliminação ou destruição segura das informações/dados, de acordo com as técnicas mais avançadas.

### 3.7 Propriedade

- A soberania dos dados e a propriedade de informações de todos os tipos que são coletadas, criadas, processadas ou disponibilizadas à Corden Pharma, conforme descrito neste documento, e a propriedade dos suportes de dados ou dispositivos de TI fornecidos pertencem exclusivamente à Corden Pharma.
- Após o vencimento ou rescisão do contrato subjacente entre o Fornecedor e a Corden Pharma, todos os dados e informações devem ser devolvidos à Corden Pharma e devem ser eliminados de forma segura dos dispositivos e suportes de armazenamento do fornecedor. Os requisitos legais (por exemplo, obrigações legais de retenção) devem ser respeitados.

### 3.9 Conformidade com a lei

O Fornecedor deve cumprir todas as leis, regulamentos e outros requisitos aplicáveis no que diz respeito à segurança da informação e cibernética, incluindo, mas não se limitando a, legislação sobre privacidade e infraestruturas críticas, e diretrizes e requisitos relacionados com as autoridades farmacêuticas.

## 4 Direito de auditoria

A Corden Pharma tem o direito de auditar o fornecedor com uma notificação prévia de sessenta (60) dias corridos, a fim de verificar o cumprimento dos presentes requisitos e a implementação das medidas acordadas. A Corden Pharma pode, a seu critério, exigir autoavaliações entre as auditorias. Em caso de violação de segurança, a Corden Pharma tem o direito de auditar o fornecedor com um aviso prévio de catorze (14) dias corridos.