1. **EICAR-Mindeststandard für Antiviren-/Anti-Malware-Produkte**
    a. Für den Antrag auf Einhaltung des EICAR-Mindeststandards muss ein Antiviren-/Anti-Malware-Produkt die folgenden Anforderungen erfüllen:
        i. Die Anforderungen dieses Standards gelten für alle Teile des Produkts, unter anderem für:
            1. den von dem Anbieter entwickelten Code,
            2. den von Dritten entwickelten und von dem Anbieter in das Produkt eingebundenen Code,
            3. den auf dem Gerät des Benutzers ausgeführten Code,
            4. Backend-Systeme, die von dem Anbieter betrieben werden, sofern sie von dem Gerät des Benutzers empfangene Daten speichern oder verarbeiten.
        ii. Der Anbieter muss über hinreichende Kenntnisse sämtlichen Codes verfügen, der in dem Produkt vorhanden ist, ob intern oder extern entwickelt, um die Einhaltung dieses Standards sicherstellen zu können.
        iii. Der Anbieter muss sämtliche Teile des in dem Produkt vorhandenen Codes, ob intern oder extern entwickelt, hinreichend kontrollieren können, um sicherzustellen, dass entdeckte Fehler, die diesem Standard entgegenstehen, unverzüglich behoben werden können.
        iv. Der Anbieter hat eine Datenschutzerklärung zu dem Produkt zu veröffentlichen. Diese Erklärung ist verständlich und umfassend und verschleiert keine relevanten Informationen. Sie enthält mindestens die an anderer Stelle in diesem Standard genannten Punkte und wird bei der Veröffentlichung neuer Produktversionen aktualisiert.
        v. Das Produkt ist so konzipiert, dass es allein die erklärten Ziele erfüllt; die erklärten Ziele werden in der Datenschutzerklärung zu dem Produkt umfassend beschrieben.
        vi. Der Anbieter unterstützt kein Programm, das die Nichterkennung von bösartigen Aktivitäten erfordert.
        vii. Das Produkt enthält keine versteckten Funktionen oder sonstige beabsichtigte Funktionen, die in den erklärten Zielen nicht vorgesehen sind.

viii Das Produkt enthält insbesondere keine „Hintertür“* und der Anbieter unterstützt kein „Third Party Access (TPA)“-Programm.

ix Das Produkt setzt kryptographische Methoden ein, um die Daten zu schützen, die mit dem Gerät ausgetauscht werden. Der Anbieter setzt kryptographische Methoden ein, um die Integrität von Code und Daten sicherzustellen, die als Teil des Produkts auf dem Gerät des Benutzers installiert werden. Alle eingesetzten kryptographischen Methoden basieren auf Algorithmen und Protokollen, die als ausreichend robust angesehen werden. Code, der kryptographische Algorithmen und Protokolle bereitstellt, basiert entweder auf weithin anerkannten Krypto-Bibliotheken oder wurde in sonstiger Weise und in hinreichender Qualität entwickelt, um ausreichend Schutz zu bieten.

x Informationen, die den Eigentümer des Gerätes, der Produktlizenz oder jede andere Person identifizieren, die das Gerät benutzt, dürfen nur aus einem zwingend notwendigen Grund an den Anbieter übermittelt werden. In der Datenschutzerklärung ist auszuführen, ob, in welchem Umfang und aus welchem Grund diese Daten übertragen werden.

xi Inhalte im Eigentum des Benutzers wie Kontakte, Nachrichten und Dokumente dürfen ohne die ausdrückliche Zustimmung des Benutzers nicht an den Anbieter übertragen werden. In der Datenschutzerklärung ist auszuführen, ob, in welchem Umfang und aus welchem Grund diese Daten übertragen werden.

xii Technische Daten – wie die Gerätekonfiguration, Informationen zu installierten und ausgeführten Anwendungen, zu Anwendungsdateien, zur Nutzung von Produkt- oder Systemfunktionen, zu installierten Updates und sonstigen vergleichbaren Daten – können zu dem Anbieter hochgeladen werden, wenn dies für die bestimmungsgemäße Verwendung des Produkts förderlich ist und wesentlichen Interessen des Benutzers nicht

entgegensteht. In der Datenschutzerklärung ist auszuführen, ob, in welchem Umfang und aus welchem Grund diese Daten übertragen werden.

xiii Alle Daten, die vom Gerät des Benutzers erhoben werden, sind nach den geltenden datenschutzrechtlichen Anforderungen geschützt. In der Datenschutzerklärung ist auszuführen, in welchem Land oder in welchen Ländern die Daten, die auf dem Gerät des Benutzers vorhanden sind, gespeichert werden dürfen.

xiv Behörden haben allein im Rahmen geltender Gesetze Zugang zu den Benutzerdaten, die bei dem Anbieter gespeichert sind.

xv Bösartiger Code und möglicherweise eingebundene Benutzerdaten werden auf Systemen des Anbieters sicher gespeichert, wodurch gewährleistet ist, dass nur berechtigte Personen auf den gespeicherten Code und die gespeicherten Daten zugreifen können.

xvi Der Austausch von bösartigem Code mit anderen berechtigten Unternehmen oder Einzelpersonen wird auf ein Mindestmaß beschränkt und erfolgt unter Einhaltung des EICAR Verhaltenskodex.

b Der Eigentümer/Anbieter des Produktes erklärt sich mit einer unabhängigen Bewertung und Überprüfung der genannten Anforderungen einverstanden.

*Nach dem EICAR Mindeststandard bedeutet „Hintertür“ jeder veröffentlichte oder nichtveröffentlichte Zugang zu der Anwendung und zu dessen Code, der nicht in den erklärten Zielen beschrieben ist.