# Erklärung des Einverständnisses mit

## den „Indispensable baseline security requirements for the procurement of secure ICT products and services“ der ENISA vom 21. Januar 2017[1]

## „CYBERSECURITY MADE IN EUROPE“

| Grundsatz | Voraussetzung | Erfüllt (Ja/Nein) | Erläuterung[2] |
|---|---|---|---|
| **Konstruktionsbedingte Sicherheit** | Der Anbieter muss das gelieferte Produkt so konstruieren und vorkonfigurieren, dass die Funktionen auf etablierten Sicherheitsverfahren basieren und auf das für den Systembetrieb strikte Minimum reduziert werden. | | |
| **Niedrigste Berechtigung** | Der Anbieter muss das Produkt gemäß dem Grundsatz der niedrigsten Berechtigung konstruieren und vorkonfigurieren, sodass Administrationsrechte nur verwendet werden, wenn sie absolut notwendig sind, die Sitzung technisch getrennt sind und alle Accounts verwaltbar sind. | | |

[1] ENISA, „Indispensable baseline security requirements for the procurement of secure ICT products and services“, 21. Januar 2017. Hier erhältlich: https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services.

[2] Bitte erläutern Sie, wie Sie diese Voraussetzung erfüllen bzw. warum Sie sie nicht erfüllen oder warum sie nicht auf Sie zutrifft, falls Sie eine bestimmte Voraussetzung nicht erfüllen.

| | | | |
|---|---|---|---|
| **Starke Authentifizierung** | Das Produkt muss Mechanismen für eine starke Authentifizierung für alle Accounts vorsehen und unterstützen. Bei einer gescheiterten Authentifizierung darf das Produkt keine benutzerspezifischen Tätigkeiten ausführen können. | | |
| **Anlagenschutz** | Das Produkt muss ein angemessenes Schutzniveau für kritische IT-Vermögenswerte während Speicherung und Übermittlung bieten. | | |
| **Sicherheit der Lieferkette** | Der Anbieter muss Mittel zur Verfügung stellen, die sicherstellen, dass das Produkt echt ist und während des Betriebs nicht manipuliert werden kann und dass seine Unversehrtheit über den gesamten Lebenszyklus des Produkts gewährleistet ist. | | |

| | | | |
|---|---|---|---|
| **Dokumententransparenz** | Der Anbieter muss umfassende und verständliche Dokumentationen zur Gesamtkonstruktion des Produkts bieten, mit Beschreibung der Architektur, Funktionen und Protokolle, ihre Realisierung durch Hardware- oder Software-Bestandteile, Schnittstellen und Interaktionen der Komponenten untereinander und mit internen und externen Diensten, um das Produkt auf möglichst sichere Weise zu implementieren und zu verwenden. | | |
| **Qualitätsmanagement** | Der Anbieter muss nachweisen können, dass ein Ansatz des Managements der konstruktionsbedingten Sicherheit angewandt wurde, einschließlich dokumentierter sicherer Softwareentwicklung, Qualitätsmanagement und Prozessen zum Management der Informationssicherheit. | | |
| **Service-Kontinuität** | Der Anbieter muss Support in einer Form gewährleisten, dass das System wie vereinbart und sicher während der vereinbarten Lebensdauer des Produkts betrieben werden kann. | | |

| | | | |
|---|---|---|---|
| **EU-Recht** | Der Anbieter muss anerkennen, dass alle Verträge und Aufträge sich auf das Recht der EU-Mitgliedstaaten beziehen und nur das Recht der EU-Mitgliedstaaten und ein Gerichtsstand in einem EU-Mitgliedstaat zur Anwendung gelangen, auch bei Subunternehmern. | | |
| **Einschränkung der Datenverwendung** | Der Anbieter muss ausdrücklich alle Datenerhebungen und Datenverarbeitungen, die stattfinden oder stattfinden können, deklarieren und kontext- und zweckbezogen begründen und dokumentieren, einschließlich der sie regelnden maßgeblichen rechtlichen Vorschriften. | | |