Schwerpunkte dieser Checkliste sind Transparenz und nahe verwandte Themen. Bereiche wie ein guter Programmierstil, schnelle Schwachstellenbehebung oder Hackerresistenz der Sicherheitssoftware selbst wurden an dieser Stelle bewusst außen vorgelassen.

	Nachvollziehbarkeit
	Sie als Verwalter einer IT-Infrastruktur besitzen die Möglichkeit, klar und einfach nachzuvollziehen:
☐	welche Daten zur Analyse aus dem Verwaltungsbereich transferiert wurden und können diese einsehen
☐	aus welchem Grund diese Daten zur Analyse hochgeladen wurden
☐	wie dringlich (z.B. Priorität) die Daten zur Analyse benötigt werden
☐	welche Ergebnisse die Analyse (in Kurzform oder Kategorien) erbracht hat
☐	inwieweit eine Löschung (z.B. Löschbestätigung) der hochgeladenen Daten beim Sicherheitsdienstleister nach der Analyse erfolgt ist
☐	Welche Daten in den Verwaltungsbereich übertragen wurden
☐	aus welchem Grund diese Daten heruntergeladen wurden
☐	welche Datenmenge (z.B. in MB) **aus** dem Verwaltungsbereich transferiert wurde
☐	welche Datenmenge (z.B. in MB) **in** den Verwaltungsbereich transferiert wurde
☐	welche sensiblen Funktionen (z.B. anfertigen eines Arbeitsspeicherauszuges eines laufenden Prozesses) aus der Ferne über die Sicherheitssoftware ausgelöst wurden
☐	aus welchem Grund diese sensiblen Funktionen ausgelöst wurden

	Steuerbarkeit
	Sie als Verwalter einer IT-Infrastruktur besitzen die Möglichkeit, sensible Funktionalitäten einfach und granular steuern zu können:
☐	Es existiert eine Steuermöglichkeit der Datenübertragungen aus dem Verwaltungsbereich *pro Datei / nach Kategorien wie dringlich der Analyst (z.B. Priorität) die Daten untersuchen will*
☐	Es existiert eine Steuermöglichkeit der aus der Ferne ausführbaren sensiblen Funktionen (z.B. Ausführung bestimmter Funktionen erst nach Freigabe durch einen internen Mitarbeiter)
☐	Steuerungsfunktionen können pro definierbarer Gruppe gesteuert werden (Bsp.: Ordnerstruktur, Dokumententyp, Benutzer, Funktionstyp)
☐	Es existiert eine sofortige Löschmöglichkeit der aus dem Verwaltungsbereich übertragenen Daten, die sich nun im Verwaltungsbereich des Sicherheitsdienstleisters befinden
☐	Es existiert eine einfache Funktion, dass Dateien, die zur Analyse hochgeladen werden sollen, zuerst eigenen Analysten vorgelegt werden. *(beispielsweise: hochsensible Daten, Daten/Programme aus der internen Softwareentwicklung)*
☐	Es existiert eine Möglichkeit, über ein konfigurierbares Regelwerk zu bestimmen, welche Daten hochgeladen bzw. nicht hochgeladen werden dürfen *(z.B. Hash, RegEx auf Dateinamen und Dateiinhalt). Regelwerk Blacklist / Whitelist*
☐	Eine Analyse ist manuell auslösbar
☐	Die Granularität der Einstellmöglichkeiten ist regelbar (idealerweise lassen sich die Einstell-Optionen je nach Nutzer-Know-how erweitern bzw. zusammenfassen: z.B. Einfach / Mittel / Expert, die jeweils dahinter liegenden Einstellungen sind umfassend dokumentiert)
☐	Die Standard-Einstellungen sind sinnvoll zwischen Sicherheit und Privacy abgewogen (hierzu existiert eine klare und verständliche Dokumentation)

	Privacy & Anonymisierung
	Sie als Verwalter einer IT-Infrastruktur besitzen die Möglichkeit nachzuvollziehen, inwieweit übertragene Daten anonymisiert / nicht anonymisiert werden:
☐	Es existiert eine Übersicht, welche Daten vor der Übertragung anonymisiert / nicht anonymisiert werden
☐	Die anonymisierten Daten sind einsehbar

	Sicherheit
	Sie als Verwalter einer IT-Infrastruktur besitzen die Möglichkeit nachzuvollziehen, dass:
☐	übertragene Daten während des Transportes angemessen verschlüsselt sind
☐	übertragene Daten im Hoheitsbereich des Sicherheitsdienstleisters verschlüsselt gespeichert werden
☐	der Sicherheitsdienstleister eine angemessen sichere Löschfunktion benutzt, so dass einmal gelöschte Daten anschließend nicht wiederherstellbar sind

	Governance
	Sie als Verwalter einer IT-Infrastruktur besitzen die Möglichkeit, Governance-Bedürfnissen in Hinblick auf den Sicherheitsdienstleister zu berücksichtigen:
☐	Eine Bestimmung des Hoheitsgebiets für die Analyse (z.B. Datenhaltung und Analysen ausschließlich innerhalb der EU) ist möglich.
☐	Eine Nachvollziehbarkeit der Zertifizierungen der Analysten (z.B. sicherheitsgeprüfte Analysten) existiert
☐	Eine Nachvollziehbarkeit von Sicherheitsprüfungen bezüglich der Analyseinfrastruktur (z.B. ISO 27001) ist gegeben
☐	Es existiert eine funktionierende Clearing-Stelle / Beschwerdestelle