Datensicherheitskonzept i.S.d. Art. 32 DSGVO (in Anlehnung an BSI-Grundschutz)

Unternehmen: PLANPROTECT AG Stand (Datum): 20.04.2026

Bearbeiter (Stefan Schuendeln / Swen Peine – IT-Leiter / Geschäftsführer AES) :

Datenschutzbeauftragter und Kontaktmöglichkeit: Antonio Morales, morales@exkulpa.de

Vertraulichkeit (Art. 32 Abs. 1 B DSGVO)	**Vorhandenes bitte ankreuzen**
Zutrittskontrolle	
Berechtigungsausweise	
Elektronische Zutrittscodekarten/ Zutrittstransponder	X
Zutrittsberechtigungskonzept	X
Videoüberwachung	X
Alarmanlage	X
Schlüsselregelung	X
Besucherausweise	
Begleitung von Besucherzutritten durch eigene Mitarbeiter	X
Anwesenheitsaufzeichnungen von Besucherzutritten	
Sicherung auch außerhalb der Arbeitszeit durch Werkschutz	
Abgestufte Sicherheitsbereiche und kontrollierter Zutritt	X
Gesicherter Eingang für An- und Ablieferung	
Kontrolle durch die Mitarbeiter (4-Augen-Prinzip)	X
Spezialverglasung	
Gesondert gesicherter Zutritt zum Rechenzentrum	X
Aufbewahrung der Server in verschlossenen Räumen	X
Aufbewahrung der Datenträger unter Verschluss bzw. in abgeschlossenen Räumen	X
Aufbewahrung von Datensicherungen (z.B. Bänder, CDs) im zutrittsgeschützten Safe	X
Anweisung zur Ausgabe von Schlüsseln	
Sonstiges **(bitte beschreiben)**	

Vertraulichkeit (Art. 32 Abs. 1 B DSGVO)	**Vorhandenes bitte ankreuzen**
Zugangskontrolle	
Verschlüsselung von Netzwerken	
● Verwendete Verschlüsselungsalgorithmen ***(bitte beschreiben)***	X
Verschluss von Datenverarbeitungsanlagen (z.B. verschlossener Cage für Server)	
Passwortsicherung von Bildschirmarbeitsplätzen	X
Funktionelle und/oder zeitlich limitierte Vergabe von Benutzerberechtigungen	X
Verwendung von individuellen Passwörtern	X
Automatische Sperrung von Nutzeraccounts nach mehrfacher Fehleingabe von Passwörtern	X
Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität (Bildschirmschoner)	X
Passwortrichtlinie mit Mindestvorgaben zur Passwortkomplexität:	X
● Passwort Mindestzeichen	12
● Groß- und Kleinschreibung, Sonderzeichen, Zahl	X
● Eingabebeschränkung bestimmter Sonderzeichen zur Verhinderung von SQL-Injections	
● Verhinderung von Trivialpasswörtern (z.B. Bello, Schatz, Familienname)	X
● Verhinderung von Passwortwechsel nach positivem Abgleich mit Wörterbüchern	
● Passworthistorie verhindert erneute Verwendung von zuvor gesetzten Passwörtern **(bitte beschreiben, ob und ab wann ein Passwort erneut verwendet werden kann)**	5
Hashing von gespeicherten Passwörtern	X
● SHA1	
● SHA2	
● SHA3	X
● bcrypt	
● Sonstige **(bitte beschreiben)**	
● Salt/Pepper Hashing (Klartext um zufällige Zeichenfolge ergänzt)	i.Vorb.
Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern	X
Prozess zum Rechteentzug bei Abteilungswechseln von Mitarbeitern	X
Prozess zum Rechteentzug bei Austritt von Mitarbeitern	X
Verpflichtung auf das Datengeheimnis nach § 5 BDSG	X
Protokollierung und Auswertung der Systembenutzung	X
Kontrollierte Vernichtung von Datenträgern	X
Programmprüfungs- und Freigabeverfahren bei Neuinstallationen	X
Aufbewahrung personenbezogener Daten in verschließbaren Sicherheitsschränken	
Sonstige **(bitte beschreiben)**	

Vertraulichkeit (Art. 32 Abs. 1A, B DSGVO)	Vorhandenes bitte ankreuzen
Zugriffskontrolle	
Festlegung der Zugriffsberechtigung, Berechtigungskonzept	X
Festlegung der Befugnis zur Dateneingabe, -änderung, -löschung	X
Trennung von Berechtigungsbewilligung (organisatorisch) und Berechtigungsvergabe (technisch)	X
Regelung zur Wiederherstellung von Daten aus Backups (wer, wann, auf wessen Anforderung)	X
Regelmäßige Überprüfung von Berechtigungen	X
Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken	X
Regelmäßige Auswertung von Protokollen (Logfiles)	X
Zeitliche Begrenzung von Zugriffsmöglichkeiten	
Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen (Read, Write, Execute)	X
Protokollierung von Dateizugriffen	X
Protokollierung von Dateilöschungen	X
Protokollierung von Dateiveränderungen	X
Eingesetzte Sicherheitssysteme (Software/Hardware):	
● Virenscanner	X
● Firewalls	X
● SPAM-Filter	X
● Intrusionprevention (IPS)	X
● Intrusiondetection (IDS)	X
● Software für das Security Information and Event Management (SIEM)	X
Beschränkter Zugriff auf LogFiles (nur Log-Admin)	X
Speicherung von Log-Files auf dediziertem LogFile-Server	i.A
Verschlüsselte Speicherung der Daten	
● verwendete Verschlüsselungsalgorithmen:	
□ AES (128/256 bit)	X
□ 3DES	
□ RSA (1024/2048 bit)	
□ Diffie-Hellmann	
□ Sonstige **(bitte beschreiben)**	
● Verwendete Hash-Funktion:	
□ SHA2 (256, 384, 512 bit)	
□ SHA3	X
□ bcrypt	
□ Sonstige **(bitte beschreiben)**	
Sonstige **(bitte beschreiben)**	

Vertraulichkeit (Art. 32 Abs. 1 B DSGVO)	Vorhandenes bitte ankreuzen
Trennungskontrolle	
Trennung von Kunden (Mandantenfähigkeit des verwendeten Systems)	X
Dateiseparierung bei Datenbanken	X
Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern)	X
Verarbeitung der Daten des Auftraggebers und anderer Kunden von unterschiedlichen Mitarbeitern des Auftragnehmers	X
Datensicherungen der Auftraggeber-Daten auf separaten Datenträgern (ohne Daten anderer Kunden)	
Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeber-Daten von Daten anderer Kunden Rechnung trägt	X
Funktionstrennung	X
Trennung von Entwicklungs-, Test- und Produktivsystem	X
Sonstige **(bitte beschreiben)**	

Integrität (Art. 32 Abs. 1 B DSGVO)	Vorhandenes bitte ankreuzen
Weitergabekontrolle	
Welche Versendungsart der Daten besteht zwischen Auftraggeber und Dritten?	
● Citrix-Verbindung (128 Bit verschlüsselt)	
● VPN-Verbindung (IP-Sec)	X
● E-Mail-Versand mit verschlüsselten ZIP-Dateien	
● Datenaustausch über https-Verbindung	X
□ verwendetes Verschlüsselungsprotokoll:	
- TLS 1.1	
- TLS 1.2	X
- TLS 1.3 (Neu)	X
● Sonstige Versendungsart **(bitte beschreiben)**	
□ verwendete Verschlüsselungsalgorithmen:	
- AES (128/256 bit)	X
- 3DES	
- RSA (1024/2048 bit)	
- Diffie-Hellmann	
- Sonstige **(bitte beschreiben)**	
□ Verwendete Hash-Funktion:	
- SHA2 (256, 384, 512 bit)	
- SHA3	
- Bcrypt	

- Sonstige **(bitte beschreiben)**	
- Salten / Pepper Hashes	
Gesicherter Eingang für An- und Ablieferung	X
Dokumentierte Verwaltung von Datenträgern, Bestandskontrolle	
Festlegung der Bereiche, in dem sich Datenträger befinden müssen	
Verschlüsselung vertraulicher Datenträger	X
Verschlüsselung von Laptopfestplatten	X
Verschlüsselung mobiler Datenträger	X
Verbot der Mitnahme von Taschen und sonstigen Gepäckstücken in die Sicherheitsbereiche	
Kontrollierte Vernichtung von Daten **(bitte beschreiben)**	X
Datenträgerentsorgung - Sichere Löschung von Datenträgern:	
● 5220.22-M-Standard des US-Verteidigungsministeriums (3-faches Überschreiben)	
● VSITR-Standard des Bundesamtes für Sicherheit und Informationstechnologie (BSI)	
● Bruce-Schneier-Algorithmus - 7faches Überschreiben	
● BSI GSHB M 2.433 (Variante 2-maliges Überschreiben davon einmal mit einem Zufallsmuster)	
● Peter-Gutmann-Algorithmus – 35-faches Überschreiben	
● Physikalische Zerstörung (z.B. Shredder bei Partikelgrößen bis max. 1000 Quadrat-Millimeter)	
● Entmagnetisierung durch thermische Zerstörung (Erhitzung der Magnetplattenoberfläche über die Curie- Temperatur der verwendeten Beschichtung hinaus (bei Eisen 766°C))	
● Entmagnetisierung mittels eines Degaussers (Magnetfeld-Stärke von mindestens 18.000 Gauss)	
● Sonstige: **HDD-Entsorgung durch RHENUS nach P-4**	
Papierentsorgung: Sicheres Vernichten von Papierdokumenten:	
● Verschlossene Behältnisse aus Metall (sog. Datenschutztonnen), Entsorgung durch Dienstleister	X
● Shredder gem. DIN 66399	X
● Sonstige Sicherheitsstufe **(bitte benennen)**	P-3
Regelung zur Anfertigung von Kopien	
Sicherungskopien von Datenträgern, die transportiert werden müssen	
Dokumentation der Stellen, an die eine Übermittlung vorgesehen ist, sowie der Übermittlungswege	
Verpackungs- und Versandvorschriften, verschlüsselter E-Mail-Versand	X
Direktabholung, Kurierdienst, Transportbegleitung	
Vollständigkeits- und Richtigkeitsprüfung	
Sonstige **(bitte beschreiben)**	

Integrität (Art. 32 Abs. 1 B DSGVO)	Vorhandenes bitte ankreuzen
Eingabekontrolle	
Kennzeichnung erfasster Daten	
Festlegung von Benutzerberechtigungen (Profile)	X
Differenzierte Benutzerberechtigungen:	X
Lesen, Ändern, Löschen	X
Teilzugriff auf Daten bzw. Funktionen	X
Feldzugriff bei Datenbanken	
Organisatorische Festlegung von Eingabezuständigkeiten	
Protokollierung von Eingaben/Löschungen	
Protokollauswertungssystem	
Verpflichtung auf das Datengeheimnis	X
Über OS-Standard hinausgehendes Log-Konzept	
Dezidierter Logserver	
Regelung der Zugriffsberechtigungen für Logserver (LogAdmin)	X
Regelung zu Aufbewahrungsfristen für Revision/Nachweiszwecke	
Sonstiges: Klicken Sie hier, um Text einzugeben.	

Integrität (Art. 32 Abs. 1 B DSGVO)	Vorhandenes bitte ankreuzen
Verfügbarkeitskontrolle	
Datensicherungs- und Backupkonzepte	X
Durchführung der Datensicherungs- und Backupkonzepte	X
Zutrittsbegrenzung in Serverräumlichkeiten auf notwendiges Personal	X
Brandmeldeanlagen in Serverräumlichkeiten	X
Rauchmelder in Serverräumlichkeiten	X
Wasserlose Brandbekämpfungssysteme in Serverräumlichkeiten	X
Klimatisierte Serverräumlichkeiten	X
Blitz-/ Überspannungsschutz	X
Wassersensoren in Serverräumlichkeiten	X
Serverräumlichkeiten in separaten Brandabschnitt	X
Unterbringung von Backupsystemen in separaten Räumlichkeiten und Brandabschnitt	X
Gewährleistung der technischen Lesbarkeit von Backupspeichermedien für die Zukunft	X
Lagerung von Archiv-Speichermedien unter notwendigen Lagerbedingungen (Klimatisierung, Schutzbedarf etc.)	
CO2 Feuerlöscher in unmittelbarer Nähe der Serverräumlichkeiten	X
Vereinbarung bzgl. Übergabe der (Daten-) Sicherungen	X
Katastrophen- oder Notfallplan (z.B. Wasser, Feuer, Explosion, Androhung von Anschlägen, Absturz, Erdbeben)	X

Einbeziehung des Einflusses angrenzender baulicher Einrichtungen	X
Schwachstellenanalyse (Geländeschutz, Gebäudeschutz, Eindringen in Rechner, Rechnernetze)	X
Aufbewahrung der Daten in Datensicherungsschränken, Tresoren	X
USV-Anlage (Unterbrechungsfreie Stromversorgung)	X
Stromgenerator	X
Sonstige **(bitte beschreiben)**	

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 B, C DSGVO)	**Vorhandenes bitte ankreuzen**
Widerstandsfähigkeits- /Ausfallsicherheitskontrolle	
Ausweich-Rechenzentren vorhanden (Hot- bzw. Cold-Stand-by?)	X
Redundante Stromversorgung	X
Redundante Datenanbindung	X
Redundante USV-Anlage	X
Redundante Stromgeneratoren	X
Redundante Klimatisierung	X
Redundante Brandbekämpfung	
sonstige redundante Systeme/Verfahren: Klicken Sie hier, um Text einzugeben.	
Festplattenspiegelung	
Einsatz einer hochverfügbaren SAN-Lösung	X
Computer Emergency Response Team (CERT)	
Loadbalancer	
Datenspeicherung auf RAID-Systemen (RAID 1 und höher)	X
Abgrenzung kritischer Komponenten	X
Durchführung von Penetrationstests	X
Systemhärtung (Deaktivierung nicht erforderlicher Komponenten)	X
Unverzügliche und regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates	X
● Identifikation der verschiedenen Geräte, aus denen sich das Netzwerk zusammensetzt, und Bestimmung ihrer Hardware-Version sowie ihrer aktuellen Software- und Firmware-Versionen.	X
● Kommunikationskanal mit den Herstellern, um sich über neue Updates und Patches zu informieren, die für die im Besitz befindlichen Geräte freigegeben wurden.	
● Definition von Zeiträumen, in denen die Updates implementiert werden sollen (z. B. Perioden niedrigerer Operationen, Wartungszeiten usw.).	
● Verwendung redundanter Systeme, um den Betrieb aufrecht zu erhalten, während die Hauptgeräte aktualisiert werden.	X
● Progressive Bereitstellung von Updates / Patches, um Probleme frühzeitig zu erkennen, ohne mehrere Geräte zu beeinträchtigen.	
● Festlegung einer Testperiode, um die korrekte Implementierung des Updates zu überprüfen und sicherzustellen, dass die Operationen mit den neuen Updates weiterhin reibungslos ablaufen.	

Sicherheit wird während der Entwurfsphase der Systeme als Hauptbetrachtung mit umfasst.	
● Definition von Sicherheitsmaßnahmen zum Schutz und zur Validierung der Kommunikation zwischen Systemkomponenten	
● Festlegen von Datenvalidierungsprozessen zwischen Geräten unter Ausschluss jeglicher unbekannten Systeme (z. B. Quellcode-Ursprungsvalidierung, MAC-Adressenfilterung usw.).	X
● Begrenzung von Berechtigungen auf Bedarfsnotwendigkeit.	X
● Widerruf vorübergehender Privilegien, sobald sie nicht mehr erforderlich sind.	
● Externe Auftragnehmer und Wartungspersonal erhalten einen spezifischen Zugang, der nur während des Eingriffs aktiv und den Rest der Zeit deaktiviert ist.	X
● Verifizierung neuer Mitarbeiter über Hintergrundkontrollen während des Inbetriebnahmeprozesses sowie Definition von Exit-Interviews beim Verlassen der Organisation.	X
● Bei der Definition von Netzwerkkommunikationstechnologien und Architektur wird auch die Interoperabilität mit einbezogen.	
● Identifizierung von Systemen, Infrastrukturen und Umgebungen, die eine Interkommunikation mit anderen Systemen (intern oder extern) erfordern, oder die diese Interkommunikation in naher Zukunft erfordern (unter Berücksichtigung des Lebenszyklus der beteiligten Geräte).	
● Auswahl von Kommunikations-Protokollen, die mit den identifizierten Systemen und den Systemen der anderen Organisationen oder Umgebungen kompatibel sind.	
● Festlegung von Brainstorming und Kommunikationskanälen für die verschiedenen Teilnehmer über den Lebenszyklus der Geräte/Software zum Austausch von Bedürfnissen und Lösungen.	
● Kollaborative Umgebungen, die den Austausch von Informationen zwischen verschiedenen Parteien ermöglichen.	
● Identifizierung und Austausch in einer gemeinsamen Plattform über potentielle Hauptangriffsvektoren.	
Periodische Sicherheitstrainings und Sensibilisierungskampagnen innerhalb der Organisation.	X
● Sensibilisierungskampagnen, um die Benutzer über die Sicherheitskonzepte zu informieren, die sowohl für konkrete Systeme als auch für traditionelle IT-Systeme spezifisch sind.	X
● Spezielles Sicherheitstraining, um zu lehren, wie man Sicherheitsmaßnahmen und Verhaltensweisen auf die täglichen Prozesse mit möglichst geringem Aufwand anwendet.	
● Triptychons, die vor neuen Bedrohungen und Risiken warnen, sowie als Erinnerung an die gemeinsamen Sicherheitspraktiken und -funktionen (ähnlich wie bei traditionellen Arbeitsplatz-Triptychonen) dienen.	
Abschluss einer Cyber-Versicherung	X
● Identifikation der IT-Geräte, Assets und Netzwerksysteme in der Infrastruktur der Organisation.	X
● Durchführung einer Risikoanalyse unter Berücksichtigung all dieser Systeme, Geräte und Vermögenswerte, die identifiziert wurden, zur Ermittlung der Bedrohungen, inklusive ihrer Wahrscheinlichkeit und ihrer Auswirkungen.	X

● Bestimmung der Sicherheitsmaßnahmen, die zur Minderung dieser Bedrohungen (direkt oder indirekt) umgesetzt werden.	X
● Auflistung der Sicherheitsmaßnahmen, die in den folgenden Monaten / Jahren umgesetzt werden sollen, um die Sicherheit dieser Geräte zu verbessern.	X
● Ermittlung des Gesamtrisikos für diese Geräte unter Berücksichtigung der anfänglichen Risikoanalyse und des Abschwächungsfaktors der vorhandenen Sicherheitsmaßnahmen (dies ergibt das Restrisiko).	X
● Festlegung, welche Risiken akzeptabel sind und welche abgedeckt werden müssen, unter der direkten Beteiligung des Top-Managements.	
● Abdeckung der Risiken, die nicht mit technischen Sicherheitsmaßnahmen ausgestattet sind, mit einer Cyber-Versicherung, welche den Umfang, die Entschädigungen und die Abdeckungsausnahmen festlegen.	X
Sonstige **(bitte beschreiben)**	

Auftragsverarbeitung (Art. 28 und Art. 32 Abs. 4 DSGVO)	**Vorhandenes bitte ankreuzen**
Auftragskontrolle	
Vertragsgestaltung gem. gesetzlichen Vorgaben (§ 62 BDSG-neu)	X
Technisch-organisatorische Maßnahmen des Dienstleisters liegen vor	X
Zentrale Erfassung und Übersicht vorhandener Dienstleister	X
Vorabkontrollen beim Auftragnehmer vor Vertragsbeginn	X
Regelmäßige Kontrollen beim Auftragnehmer nach Vertragsbeginn (während Vertragsdauer)	X
Vor-Ort-Kontrollen beim Auftragnehmer	
Überprüfung des Datensicherheitskonzepts beim Auftragnehmer	X
Sichtung vorhandener IT-Sicherheitszertifikate der Auftragnehmer	X
Erteilung von Weisungen zur Verbesserung des Datenschutzes ggü. Auftragnehmer möglich	
Sonstige **(bitte beschreiben)**	

Überprüfung, Bewertung und Evaluierung von getroffenen Maßnahmen (Art. 32 Abs. 1 D DSGVO)	**Vorhandenes bitte ankreuzen**
Kontrollverfahren	
Regelmäßige Aktualisierung der Verzeichnisse von Verarbeitungstätigkeiten (VVT)	X
Regelmäßige Überprüfung der technisch-organisatorischen Maßnahmen	X
Regelmäßige Überprüfung von Datenverarbeitungsprozessen inkl. Dokumentation	X
Prozess zur Wahrung von Betroffenenrechte	X
Prozess zum Umgang mit Datenschutzvorfällen	X
Regelung zur Einbeziehung des Datenschutzbeauftragten bei der Implementierung neuer oder Änderung bestehender Datenverarbeitungsverfahren	X
Datenschutzfreundliche Voreinstellungen (privacy by design / privacy by default) bei Datenverarbeitungssystemen	X

Security Intelligence unter Verwendung von:	
● Indicators of compromise (IOC)	
● Structured Threat Information eXpression (STIX)	
● Trusted Automated eXchange of Indicator Information (TAXII)	
● Cyber Observable eXpression (Cybox)	
● YARA	
Sonstige **(bitte beschreiben)**	

Zertifizierungen und nationale/internationale Standards: **(*Bitte Belege beifügen*)**	**Vorhandenes bitte ankreuzen**
Zertifizierung nach ISO 27001	
Zertifizierung nach ISO 27002	
Zertifizierung nach IDW PS 330	
Zertifizierung nach IDW RS FAIT 1	
Zertifizierung nach BSI-Standard 100-3 (Notfallmanagement)	
Datenschutzzertifikat / Datenschutzprüfsiegel (gemäß Art. 42 EU-DSGVO)	
Genehmigte Verhaltensregeln (gemäß Art. 40 EU-DSGVO)	
Verifizierte verbindliche interne Datenschutzvorschriften (Binding Corporate Rules) (Gemäß Art. 47 EU-DSGVO)	