Sicherheitskonzept (technisch-organisatorische Maßnahmen) gemäß Art. 32 DS-GVO bei der PLANPROTECT AG

Unternehmen: PLANPROTECT AG Stand: April 2018

Datenschutzbeauftragter und Kontaktmöglichkeit: Markus Weuthen, weuthen@eu-con.net, 02452/993311

Vertraulichkeit (Art. 32 Abs. 1 b DS-GVO)	Getroffene Maßnahmen
Zutrittskontrolle	
Elektronische Zutrittscodekarten/ Zutrittstransponder	X
Zutrittsberechtigungskonzept	X
Videoüberwachung	X
Alarmanlage	X
Schlüsselregelung	X
Begleitung von Besucherzutritten durch eigene Mitarbeiter	X
Abgestufte Sicherheitsbereiche und kontrollierter Zutritt	X
Kontrolle durch die Mitarbeiter (4-Augen-Prinzip)	X
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

Vertraulichkeit (Art. 32 Abs. 1 b DS-GVO)	Getroffene Maßnahmen
Zugangskontrolle	
Verschluss von Datenverarbeitungsanlagen (verschlossener Cage für Server)	X
Passwortsicherung von Bildschirmarbeitsplätzen	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
● mindestens 12 Zeichen	X
● Groß- und Kleinschreibung, Sonderzeichen, Zahl	X
● Eingabebeschränkung bestimmter Sonderzeichen zur Verhinderung von SQL-Injections	X
● Passwortwechsel nach 120 Tagen	X
● Verhinderung von Trivialpasswörtern (z.B. Bello, Schatz, Familienname)	X
● Verhinderung von Passwortwechsel nach positivem Abgleich mit Wörterbüchern	X
● Passworthistorie von drei Monaten verhindert erneute Verwendung von zuvor gesetzten Passwörtern	X
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 § 53 BDSG	X
Kontrollierte Vernichtung von Datenträgern	X

Aufbewahrung personenbezogener Daten in verschließbaren Sicherheitsschränken	X

Vertraulichkeit (Art. 32 Abs. 1a, b DS-GVO)	Getroffene Maßnahmen
Zugriffskontrolle	
Festlegung der Zugriffsberechtigung, Berechtigungskonzept	X
Festlegung der Befugnis zur Dateneingabe, -änderung, -löschung	X
Regelung zur Wiederherstellung von Daten aus Backups (wer, wann, auf wessen Anforderung)	X
Regelmäßige Überprüfung von Berechtigungen einmal pro Quartal	X
Regelmäßige Auswertung von Protokollen (Logfiles) einmal pro Quartal	X
●Virenscanner	X
● Firewalls	X
●SPAM-Filter	X
● Intrusionprevention (IPS)	X
● Intrusiondetection (IDS)	X
Beschränkter Zugriff auf LogFiles (nur Log-Admin)	X
Speicherung von Log-Files auf dediziertem LogFile-Server	X
Verschlüsselte Speicherung der Daten	X
□ AES (128/256 bit)	X
● Verwendete Hash-Funktion:	
□ SHA2 (256, 384, 512 bit)	X

Vertraulichkeit (Art. 32 Abs. 1 b DS-GVO)	Getroffene Maßnahmen
Trennungskontrolle	
Trennung von Kunden (Mandantenfähigkeit des verwendeten Systems)	X
Dateiseparierung bei Datenbanken	X
Logische Datentrennung auf Basis von Kundennummern	X
Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeber-Daten von Daten anderer Kunden Rechnung trägt	X
Trennung von Entwicklungs-, Test- und Produktivsystem	X

Integrität (Art. 32 Abs. 1 b DS-GVO)	Getroffene Maßnahmen
Weitergabekontrolle	
Versendungsart der Daten zwischen Auftraggeber und Dritten:	
● VPN-Verbindung (IP-Sec)	X
● E-Mail Versand mit verschlüsselten ZIP-Dateien	X
Verschlüsselung von Laptopfestplatten	X
Kontrollierte Vernichtung von Daten mittels DBAN	X
Datenträgerentsorgung - Sichere Löschung von Datenträgern:	X
● BSI GSHB M 2.433 (Variante 2-maliges Überschreiben davon einmal mit einem Zufallsmuster)	X
Papierentsorgung: Sicheres Vernichten von Papierdokumenten:	X

● Shredder gem. DIN 66399	X

Integrität (Art. 32 Abs. 1 b DS-GVO)	Getroffene Maßnahmen
Eingabekontrolle	
Festlegung von Benutzerberechtigungen (Profile)	X
Organisatorische Festlegung von Eingabezuständigkeiten	X
Verpflichtung auf das Datengeheimnis	X

Integrität (Art. 32 Abs. 1 b DS-GVO)	Getroffene Maßnahmen
Verfügbarkeitskontrolle	
Datensicherungs- und Backupkonzepte	X
Zutrittsbegrenzung in Serverräumlichkeiten auf notwendiges Personal	X
Wasserlose Brandbekämpfungssysteme in Serverräumlichkeiten	X
Klimatisierte Serverräumlichkeiten	X
Wassersensoren in Serverräumlichkeiten	X
Unterbringung von Backupsystemen in separaten Räumlichkeiten und Brandabschnitt	X
CO2 Feuerlöscher in unmittelbarer Nähe der Serverräumlichkeiten	X
USV-Anlage (Unterbrechungsfreie Stromversorgung)	X

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 b, c DS-GVO)	Getroffene Maßnahmen
Widerstandsfähigkeits- /Ausfallsicherheitskontrolle	
Datenspeicherung auf RAID-Systemen (RAID 1 und höher)	X
Systemhärtung (Deaktivierung nicht erforderlicher Komponenten)	X
Unverzügliche und regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates	X
● Externe Auftragnehmer und Wartungspersonal erhalten einen spezifischen Zugang, der nur während des Eingriffs aktiv und den Rest der Zeit deaktiviert ist.	X
● Identifikation der IT-Geräte, Assets und Netzwerksysteme in der Infrastruktur der Organisation.	X

Auftragsverarbeitung (Art. 28 und Art. 32 Abs. 4 DS-GVO)	Getroffene Maßnahmen
Auftragskontrolle	
Vertragsgestaltung gem. gesetzlichen Vorgaben (§ 62 BDSG-neu)	X
Technisch-organisatorische Maßnahmen des Dienstleisters Protego (Leitstelle) liegen vor	X
Zentrale Erfassung und Übersicht vorhandener Dienstleister	X
Regelmäßige Kontrollen beim Auftragnehmer nach Vertragsbeginn (während Vertragsdauer)	X

Überprüfung, Bewertung und Evaluierung von getroffenen Maßnahmen (Art. 32 Abs. 1 d DS-GVO)	Getroffene Maßnahmen
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