Verzeichnis von Verarbeitungstätigkeiten PISA sales GmbH	PisaSales	
Sicherheit der Verarbeitung (verarbeitungsübergreifende technische und organisatorische Maßnahmen)	Version	0.5
	letzte Änderung	3/25/21

Maßnahmen zur Sicherheit der Datenverarbeitung

A Maßnahmen zur Pseudonymisierung

Maßnahmen, die den unmittelbaren Personenbezug während der Verarbeitung in einer Weise reduzieren, dass nur mit Hinzuziehung zusätzlicher Informationen eine Zuordnung zu einer spezifischen betroffenen Person möglich ist. Die Zusatzinformationen sind dabei durch geeignete technische und organisatorische Maßnahmen von dem Pseudonym getrennt aufzubewahren:
Generalisierung (x-en) durch eigenen Programmcode

B Maßnahmen zur Verschlüsselung

Maßnahmen oder Vorgänge, bei denen ein klar lesbarer Text / Information mit Hilfe eines Verschlüsselungsverfahrens (Kryptosystem) in eine unleserliche, das heißt nicht einfach interpretierbare Zeichenfolge (Geheimtext) umgewandelt wird:
Passwortverschlüsselung über „bCrypt“ mit „Salz und Pfeffer“, basierend auf dem Blowfish-Algorithmus.

C Maßnahmen zur Sicherung der Vertraulichkeit

Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, sowie zu vertraulichen Akten und Datenträgern physisch verwehren:
Eingangskontrolle (Objektzutritt nach Klingel und Türsummer); Elektronisches Zutrittskontrollsystem Büroräume und Empfangsbereich mit RFID-Chipkarte und PIN; Gesonderter Empfangsbereich; Besucherbegleitung; Notfall-Knopf an der Telefonanlage für Empfangspersonal zur "stummen" Anforderung von Mitarbeitern bei Gefahrensituationen im Empfangsbereich; Gesonderter Sicherheitsbereich (z.B. Serverraum); Alarmanlage mit Aufschaltung Sicherheitsdienstleister 24/7; Protokollierte Ausgabe von Schlüsseln und Chipkarten; Videoüberwachung 24/7- Sicherheitspersonal (Rechenzentrum)

Maßnahmen, die den Zugang zur Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte verwehren, sowie Maßnahmen zur Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte:
Personifizierte Nutzererkennungen; Einrichtung eines Benutzerstammsatzes pro User; Kennwortverfahren gemäß dokumentierter interner Kennwortrichline; Authentifizierungsverfahren; Active Directory; Kennwortzertifikate (LINUX); Automatische Sperrung von Arbeitsplätzen bei Inaktivität, Kennwort bei Wiederaufnahme; Begrenzung der Zahl der berechtigten Mitarbeiter bei sensiblen Datenverarbeitungsvorgängen; Verschlüsselung von Datenträgern; Core Firewall; Abkapselung von sensiblen Systemen durch getrennte Netzbereiche; Protokollierung der Anmeldeversuche und Abbruch des Anmeldevorgangs nach festgelegter Zahl (3 Fehleingaben) von erfolglosen Anmeldeversuchen; Protokollierung Passworthistorie gegen Wiederverwendung; Regelmäßig aktualisierte Antiviren- und Spywarefilter.

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren berechtigten Personen ausschließlich auf die ihrer Zugriffsberechtigung umfassten personenbezogenen Daten Zugang haben, sodass Daten bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können:
Protokollierung von Zugriffen und Missbrauchsversuchen; Benutzerverwaltung und Rechtekonzept (insbesondere File-Server); zertifikatsbasierte Zugriffsberechtigungen; Datenträgerverwaltung; Abschließbare Container an den Arbeitsplätzen; Dokumentierte Benutzerverwaltung und Rechtekonzept (PisaSales CRM); Berechtigungsvergabe auf Ebene von Rollen, Profilen, Gruppen und Feldern (PisaSales CRM); Individuelle Steuerung des Datensatzzugriffs durch den Eigentümer für Gruppen oder einzelne Benutzer (PisaSales CRM); Sicherung der referentiellen Integrität, Zugriffsschutz und Locking (PisaSales CRM); LDAP-Anbindung (PisaSales CRM); Verschlüsselung von Notebooks, Smartphones, USB Sticks und sonstigen mobilen Datenträgern (VeraCrypt 1.21 by IDRIX)

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist:
Berechtigungskonzepte; System aus Lese- und Schreibberechtigungen für Installations-Ordner; Abgetrenntes Gäste-WLAN; Trennung von Test- und Produktivsystemen; Separierte Datenbanken/ Instanzen für jeden Kunden (PisaSales CRM); Getrennte Definition von Datenobjekten und Präsentationsobjekten (Repository-Technologie, PisaSales CRM), Softwareseitige Trennung Kunden, Partner, Lieferanten etc. durch Gruppen, Kategorien, Kennzeichnung

D Maßnahmen zur Sicherung der Integrität

Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden:
Update-/Upgradeprozess durch Einspielen neuer Releases und Patchtes mit Release-/Patchmanagement; Funktionstests vor und bei der Kundeninstallation;

Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können:
4-Augen-Prinzip mit Kundenunterstützung bei Wartungsmaßnahmen (PisaSales CRM); Aufarbeitung von Datenbankabfragen im Server und Rückgabe von Anfragen/Suchergebnissen in aufbereiteter Form mit definiertem Datenumfang zur Verhinderung von SQL-Injections (PisaSales CRM); Logging; Prüfsummen

Maßnahmen, die gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden:
Übermittlung von Daten über verschlüsselte Container oder Tunnelverbindungen; Firewallsysteme; HTTPS-Verschlüsselung (PisaSales CRM); Optional VPN-Zugriff in geschütztem Unternehmensnetzwerk möglich (PisaSales CRM); Entsorgungsdienstleister zur professionellen Aktenvernichtung; Transportprozesse mit individueller Verantwortlichkeit; sicherer Transportbehälter für Datenträger; umfassende Protokollierungsverfahren; Transportprozesse mit individueller Verantwortlichkeit

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierten Verarbeitungssystemen eingegeben oder verändert worden sind:
Protokollierung wesentlicher Systemaktivitäten und Aufbewahrung dieser Protokolle; Protokollauswertungssysteme; Protokollierungsmonitor (PisaSales CRM); Protokollieren von Datensatzänderungen über Journal (PisaSales CRM); Protokollieren auf Feldebene und attributbezogene Bewertung der Datenqualität (PisaSales CRM)

E Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:
Zutrittsgesicherter Serverraum; Datensicherungsverfahren; Räumliche Trennung von Datensicherungsverfahren; regelmäßige Tests der Datenwiederherstellung; Daten in relationaler Datenbank (PisaSales CRM); Virtualisierte Systeme mit VMWare (mit Support); Brandschutzzonen, Wasser- und Brandfrühwarnsystem, hochverfügbare Klimatechnik, Luftfeuchteregelanlage (Rechenzentrum); Unterbrechungsfreie redundante Stromversorgungen; Notstromaggregate (Rechenzentrum); Überspannungsschutz (Rechenzentrum); Direkte Aufschaltung bei der örtlichen Feuerwehr (Rechenzentrum)

Maßnahmen, die die Fähigkeit sicherstellen, die Verfügbarkeit der personenbezogenen Daten, der eingesetzten Systeme und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen:
Regelmäßige automatische Datenbanksicherungen und Backups durch IT-Abteilung; Recovery- und Desastermanagement-Tests, Penetrationstests; regelmäßige Tests der Datenwiederherstellung

Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden:

Automatisches Monitoring (ZABBIX) mit Online-Benachrichtigung; Eskalationsmanagement; Befehlskette; IT-Bereitschaft 24/7; Standby-Support 9-17 mit Service Level Agreement; Recovery- und Desastermanagement-Tests

F Maßnahmen zur regelmäßigen Evaluation der Sicherheit der Datenverarbeitung

Maßnahmen, die die datenschutzkonforme und sichere Verarbeitung sicherstellen:
Datenschutzfreundliche Voreinstellungen; internes Datenschutzmanagement; Risikoanalyse durch externen Datenschutzbeauftragten (Risk Assessment); Datenschutzfolgeabschätzung bei Einführung/ Verwendung neuer Technologien; Vertragsgebundene Auftragsverarbeitung, Auftragskontrolle; Formalisierte Prozesse für Datenschutzvorfälle; regelmäßige Instruktion und Schulung der Mitarbeiter zu Datenschutzrichtlinien und formalisierten Prozessen;

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:
Formalisiertes Auftragsmanagement; Vertragsgebundenes Auftragsverarbeitungsmanagement (AV-Verträge); Festlegung von Weisungsbefugnissen; Weisungen des Auftraggebers werden dokumentiert, Kontrollrechte bei Auftragsverarbeitern;