

Datenschutz-Vereinbarung für das Durchführen von Sicherheitsuntersuchungen, Sicherheitsmonitoring, Bug Bounty Dienstleistungen und Forensischen Ermittlungen

zwischen dem

Kunden, welcher im Einzelvertrag
unter Vertragsparteien erwähnt ist

(nachfolgend "Auftraggeber" genannt)

und der

Compass Security Deutschland GmbH
Lietzenburger Straße 75
DE-10719 Berlin
Deutschland

(nachfolgend "Auftragnehmer" genannt)

1 Datenschutz-Vereinbarung

1.1 Präambel

Der Auftragnehmer führt für den Auftraggeber entsprechend des zwischen diesen Parteien bestehenden Vertrags "Leistungsvereinbarung" Sicherheits-, Prüf- und Testarbeiten durch. Dabei werden im Auftrag IT-Systeme sicherheitstechnisch geprüft und auf Schwachstellen untersucht. Es ist möglich, dass der Auftragnehmer im Zuge dieser Arbeiten in Kontakt mit Personendaten unter der Kontrolle des Auftraggebers gelangen könnte.

Die Parteien stellen fest, dass deshalb abhängig von der Gerichtsbarkeit des Auftraggebers, die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung "DS-GVO") oder das Schweizer Bundesgesetz über den Datenschutz ("DSG" oder zusammen mit DS-GVO "Datenschutzgesetz") grundsätzlich Anwendung auf das Auftragsverhältnis finden könnte. Daher einigen sich die Parteien, dass eine mögliche, allerdings nicht beabsichtigte Verarbeitung von personenbezogenen Daten auf der Grundlage dieser Datenschutzvereinbarung ("DVA") erfolgt, welcher die Bestimmungen der Datenschutzgesetze berücksichtigt.

1.2 Gegenstand

Die vom Auftragnehmer durchgeführten Datenverarbeitungsaktivitäten ergeben sich aus dem Dienstleistungsvertrag zwischen dem Auftraggeber und dem Auftragnehmer.

Im Rahmen der Untersuchungen und Testaktivitäten werden unter anderem Angriffsversuche auf die Systeme des Auftraggebers durchgeführt, kompromittierte Systeme analysiert sowie forensische Untersuchungen vorgenommen. Der Auftragnehmer versucht, Schwachstellen in den Systemen und der dazugehörigen Organisation zu finden und aufzuzeigen. Dabei wird auf Datenbestände des Auftraggebers zugegriffen und diese werden analysiert. Aufgrund der Natur dieser Tätigkeiten können verschiedene Arten von Daten absichtlich oder versehentlich eingesehen werden, darunter auch personenbezogene Daten.

Die Leistungsvereinbarung wie auch diese Datenschutz-Vereinbarung enthalten keinen expliziten Auftrag des Auftraggebers an den Auftragnehmer zur Verarbeitung von Personendaten nach Art. 4 und 28 DS-GVO (Art. 5 und Art. 9 DSG).

Es ist jedoch möglich, dass Personendaten nach Definition von Art. 4 DS-GVO (Art. 5 DSG) im Rahmen der Prüfungsaktivitäten verarbeitet werden. Aus diesem Grund wird die potenzielle Verarbeitung dieser Daten und die Beziehung zwischen Auftraggeber und Auftragnehmer in dieser Datenschutz-Vereinbarung gemäss Art. 28 DS-GVO (Art. 9 DSG) geregelt.

Der Auftraggeber nimmt zur Kenntnis, dass der Auftragnehmer im Rahmen der Erbringung der Dienstleistungen personenbezogene Daten verarbeiten kann.

1.3 Dauer

Die Dauer dieses Auftrags entspricht der Laufzeit der Leistungsvereinbarung.

1.4 Konkretisierung des Auftragsinhaltes

Der Gegenstand des Auftrags ist detailliert im oben erwähnten Vertrag im Kapitel "Projektbeschreibung" beschrieben.

Art und Zweck der Verarbeitung: Der Auftragnehmer erbringt für den Auftraggeber IT-Sicherheits- und Penetrationstests, Sicherheitsmonitoring, digitale Forensik, Incident Response oder Bug Bounty Dienstleistungen und kann in diesem Zusammenhang personenbezogene Daten des Auftraggebers gemäss dessen Weisungen verarbeiten. Auf Grund der Natur der Leistungsvereinbarung ist es nicht möglich, vor der Auftragsausführung Aussagen zu den möglicherweise bearbeiteten Personendaten zu machen.

Art der personenbezogenen Daten: Die personenbezogenen Daten, die verarbeitet werden können, sind diejenigen, die sich in der Umgebung des Auftraggebers befinden. Dies kann Namen und die Kontaktdaten von Mitarbeitenden, Kunden und Mitgliedern des Auftraggebers umfassen, ist aber nicht darauf beschränkt.

Es kann nicht ausgeschlossen werden, dass auch besonders schützenswerte Personendaten nach Art. 9 DS-GVO (bzw. wie in Art. 5 DSGVO definiert) vom Auftragnehmer eingesehen oder verarbeitet werden. Der Auftraggeber bestätigt, dass er in einem solchen Fall seinen Pflichten gegenüber den betroffenen Personen gemäss den anwendbaren Datenschutzgesetzen nachgekommen ist.

Sollten besonders schützenswerte Personendaten involviert sein, informiert der Auftraggeber den Auftragnehmer vor der Ausführung des Auftrags und instruiert ihn bezüglich der zu treffenden Massnahmen.

Kategorien von betroffenen Personen: Von einer möglichen Verarbeitung können insbesondere die Mitarbeiter des Auftraggebers, seine Kunden und Mitglieder betroffen sein.

1.5 Technische / Organisatorische Massnahmen

Der Auftragnehmer stellt sicher, dass möglicherweise zu ihm gelangende Personendaten ausreichend geschützt sind (siehe Anlage 1).

- 1) Der Auftragnehmer hat die Sicherheit gem. Art. 28,32 DS-GVO (Art. 8,9 DSGVO), insbesondere in Verbindung mit Art. 5 DS-GVO (Art. 6 DSGVO) herzustellen. Insgesamt handelt es sich bei den zu treffenden Massnahmen um Massnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO (Art. 8 DSGVO) zu berücksichtigen (Einzelheiten in Anlage 1).
- 2) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Massnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber auf Verlangen zur Durchsicht zu übergeben (siehe Anlage 1). Durch die Unterzeichnung dieser Vereinbarung werden die dokumentierten Massnahmen gemäss Anlage 1 Grundlage des Auftrags. Soweit die Prüfung oder ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
- 3) Die technischen und organisatorischen Massnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Massnahmen umzusetzen. Dabei darf das festgelegte Sicherheitsniveau nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

1.6 Verarbeitung von Daten und Betroffenenrechte

- 1) Der Auftragnehmer hat keinen ausdrücklichen Auftrag, personenbezogene Daten zu verarbeiten. Im Rahmen der Sicherheitsuntersuchungen ist es jedoch möglich, dass Personendaten durch Mitarbeiter des Auftragnehmers offengelegt und temporär, für die Dauer des Vertrages oder wie in der Dienstleistungsvereinbarung festgelegt, gespeichert werden. Diese Daten dienen zur Dokumentation der Prüfergebnisse sowie zur Nachvollziehbarkeit des Prüfablaufs. Eine weitergehende Verarbeitung ist ausgeschlossen.
- 2) Der Auftragnehmer löscht Personendaten unverzüglich, welche für die Durchführung der Testaktivitäten oder deren Auswertung nicht benötigt werden. Alternativ kann er diese Daten anonymisieren.
- 3) Alle Betroffenenrechte müssen beim Auftraggeber geltend gemacht werden. Der Auftragnehmer erteilt keine direkten Auskünfte an Betroffene. Er erteilt keinerlei Auskünfte über Existenz oder Inhalt des Auftrags oder die Inhalte der Leistungsvereinbarung.

1.7 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäss DS-GVO oder DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- 1) Die Wahrung der Vertraulichkeit gemäss Art. 28 Abs. 3 S. 2 lit. b, Art. 29, 32 Abs. 4 DS-GVO (Art. 8 DSGVO). Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschliesslich entsprechend der Weisung des Auftraggebers verarbeiten einschliesslich den in der Leistungsvereinbarung und dieser Datenschutz-Vereinbarung eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- 2) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Massnahmen gemäss Art. 28 Abs. 3 Satz 2 lit. c, 32 DS-GVO (Einzelheiten in Anlage 1) (Art. 7 DSGVO).
- 3) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- 4) Der Auftragnehmer kontrolliert regelmässig die internen Prozesse sowie die technischen und organisatorischen Massnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- 5) Nachweisbarkeit der getroffenen technischen und organisatorischen Massnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 1.9 dieser Vereinbarung.
- 6) Der Auftragnehmer kann im Regelfall auf Grund der fehlenden Informationslage zu den Prüfdaten kein Verarbeitungsverzeichnis gemäss Art. 30 DS-GVO (Art. 12 DSGVO) führen.

Als Datenschutzbeauftragter wird benannt:

Dr. Sarah Weiss
Paulstrasse 13
DE-67346 Speyer
Tel. +49 623 23185490
Mail: privacy@compass-security.com

1.8 Unterauftragsverhältnisse

- 1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Massnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmassnahmen zu ergreifen.
- 2) Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen in Bezug auf neue Unterauftragnehmer oder Ersetzen bestehender Unterauftragnehmer. Dies gibt dem Auftraggeber die Möglichkeit, solchen Änderungen zu widersprechen (Art. 28 Abs. 2 Satz 2 DS-GVO). Die in Anlage 3 aufgeführten Unterauftragnehmer gelten als genehmigt.

- 3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
- 4) Erbringt der Unterauftragnehmer die vereinbarte Leistung ausserhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Massnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen. Ein angemessenes Datenschutzniveau wurde von der EU-Kommission in einer förmlichen Entscheidung für die Schweiz festgestellt: 2000/518/EC (obwohl es sich um einen veralteten Angemessenheitsbeschluss handelt, wurde im Dezember 2024 bestätigt, dass dieser noch in Kraft ist).

1.9 Kontrollrechte des Auftraggebers

- 1) Der Auftraggeber hat das Recht, in Abstimmung mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
- 2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Massnahmen nachzuweisen.
- 3) Der Nachweis solcher Massnahmen, kann erfolgen durch
 - a) Direkte Prüfung durch den Auftraggeber;
 - b) die Einhaltung genehmigter Verhaltensregeln gemäss Art. 40 DS-GVO (Art. 11 DSGVO);
 - c) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäss Art. 42 DS-GVO (Art. 13 DSGVO);
 - d) die Einhaltung verbindlicher Datenschutz-Vorschriften im Konzernverbund gemäss Art. 47 DS-GVO (vgl. Art. 15, Abs. 2 Satz 4);
 - e) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
 - f) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz);
 - g) Entstehen beim Auftragnehmer durch die Ausübung der Kontrollrechte und durch die Erbringung der geforderten Nachweise unerwartete Kosten, kann der Auftragnehmer eine angemessene Vergütung vom Auftraggeber verlangen.

1.10 Mitteilung bei Verstössen des Auftragnehmers

- 1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO (Art 8, 22 - 24 DSGVO) genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.
 - a) die Meldung, dass auf personenbezogene Daten zugegriffen werden konnte
 - b) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Massnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
 - c) die Verpflichtung, Verletzungen personenbezogener Daten an den Auftraggeber zu melden
 - d) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen zur Verfügung zu stellen
 - e) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgeabschätzung
 - f) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde
- 2) Für alle Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine angemessene Vergütung beanspruchen.

1.11 Weisungsbefugnis des Auftraggebers

- 1) Mündliche Weisungen bestätigen beide Parteien unverzüglich (mind. Textform).
- 2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstosse gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

1.12 Löschung und Rückgabe von personenbezogenen Daten

- 1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemässen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
- 2) Daten, welche für die Dokumentation der Prüfung und der Nachvollziehbarkeit der Arbeiten notwendig sind, werden solange gespeichert, wie dies für den jeweiligen Auftrag notwendig ist. Der Auftraggeber kann verlangen, dass Daten nach Abschluss der Prüfung gelöscht werden. Der Auftragnehmer führt die Löschung durch, sofern nicht zwingende gesetzliche Gründe für eine Speicherung vorliegen. Ohne nachvollziehbare Instruktion des Auftraggebers werden Daten nach 5 Jahren nach abgeschlossener Prüfung gelöscht.
- 3) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber - spätestens mit Beendigung der Leistungsvereinbarung - hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
- 4) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemässen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Ende der Leistungsvereinbarung hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

1.13 Schlussbestimmungen

- 1) Diese Vereinbarung ersetzt keine bisher geschlossenen Vereinbarungen.
- 2) Nebenabreden oder Änderungen dieses Auftrags bedürfen der Schriftform.
- 3) Bezugnahmen auf Gesetze, Vorschriften, Dokumente und Anhänge gelten, soweit nicht ausdrücklich etwas anderes bestimmt ist, für die Gesetze, Vorschriften, Dokumente und Anhänge in ihrer jeweils geltenden Fassung, also einschliesslich etwaiger Änderungen nach dem Datum dieser Vereinbarung.
- 4) Die Anhänge sind integraler Bestandteil dieser Vereinbarung. Im Falle eines Widerspruchs zwischen den Bestimmungen des eigentlichen Vereinbarungstextes und seiner Anhänge, gehen die Bestimmungen der Vereinbarung vor. Zwingende gesetzliche Vorschriften bleiben hiervon jedoch unberührt.
- 5) Sollten einzelne Bestimmungen dieses Auftrags unwirksam oder undurchführbar sein oder werden, so wird dadurch die Wirksamkeit der übrigen Teile nicht berührt. Die Parteien verpflichten sich in einem solchen Falle, die unwirksame oder undurchführbare Bestimmung durch eine solche zu ersetzen, die dem angestrebten Zweck in rechtlich zulässiger Weise möglichst nahekommt, gleiches gilt bei Regelungslücken. Im Falle eines Widerspruchs zwischen datenschutzrelevanten Inhalten dieser Datenschutz-Vereinbarung mit der Leistungsvereinbarung oder den AGB gehen die Bestimmungen dieser Vereinbarung vor.

- 6) Der Auftraggeber bestätigt, dass er der Verantwortliche ist und daher die Bestimmungen der geltenden Datenschutzgesetze einhält und keine Inhalte zur Verarbeitung anbietet, welche die Verletzung der Persönlichkeitsrechte von Betroffenen bedeuten könnte.
- 7) Im Aussenverhältnis haftet der Auftraggeber gemäss den datenschutzrechtlichen Haftungsbestimmungen für den Schaden, der durch eine nicht gesetzeskonforme Verarbeitung verursacht wurde. Der Auftragnehmer haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen Verpflichtungen aus dieser Vereinbarung nicht nachgekommen ist oder gegen die Instruktionen des Auftraggebers gehandelt hat. Es gelten die Haftungsbestimmungen der Leistungsvereinbarung und den AGB.

Anlage 1

Technische / Organisatorische Massnahmen

1. Vertraulichkeit

Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen:

- Magnet- oder Chipkarten
- Schlüssel
- elektrische Türöffner
- Werkschutz bzw. Pförtner
- Alarmanlagen
- Videoanlagen
- Automatisches Zugangskontrollsystem
- Schliesssystem mit Codesperre
- Manuelles Schliesssystem
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal
- Sorgfältige Auswahl von Wachpersonal
- Tragepflicht von Berechtigungsausweisen
- Besucher werden beaufsichtigt
- Jeder kennt jeden (KMU)

Zugangskontrolle

Keine unbefugte Systembenutzung:

- (sichere) Kennwörter
- automatische Sperrmechanismen
- Zwei-Faktor-Authentifizierung
- Verschlüsselung von Datenträgern
- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Authentifikation mit Benutzername / Passwort
- Gehäuseverriegelungen
- Einsatz von VPN-Technologie
- Sperren von externen Schnittstellen (USB etc.)
- Verschlüsselung von mobilen Datenträgern
- Verschlüsselung von Smartphone-Inhalten
- Einsatz von zentraler Smartphone-Administrations-Software
- Einsatz von Anti-Viren-Software
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Einsatz einer Hardware/Software-Firewall

Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems

- Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte
- Protokollierung von Zugriffen
- Erstellen eines Berechtigungskonzepts
- Verwaltung der Rechte durch Systemadministrator
- Reduzierung der Anzahl der Administratoren
- Passworrichtlinie inkl. Passwortlänge, Passwortwechsel
- Sichere Aufbewahrung von Datenträgern
- Sicheres Wipen von Datenträgern vor Wiederverwendung
- Ordnungsgemässe Vernichtung von Datenträgern (DIN 66399)
- Verschlüsselung von Datenträgern

Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden:

- Sandboxing
- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Softwarebasierte Mandantentrennung
- Erstellung eines Berechtigungskonzepts
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei
- Festlegung von Datenbankrechten

Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Massnahmen unterliegen.

2. Integrität

Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

- Verschlüsselung
- Virtual Private Networks (VPN)
- elektronische Signatur
- Weitergabe von personenbezogenen Daten in anonymisierter oder pseudonymisierter Form
- Erstellen einer Übersicht von regelmässigen Abruf- und Übermittlungsvorgängen
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschrufen
- Beim physischen Transport: sichere Transportbehälter/-verpackungen

Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Protokollierung der Eingabe, Änderung und Löschung personenbezogener Daten

- Dokumentenmanagement
- Erstellen einer Übersicht, mit welchen Applikationen welche personenbezogenen Daten eingegeben, geändert und gelöscht werden können.
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung personenbezogener Daten durch individuelle Benutzernamen
- Aufbewahrung von Formularen, von denen personenbezogene Daten in automatisierte Verarbeitungen übernommen worden sind
- Vergabe von Rechten zur Eingabe, Änderung und Löschung personenbezogener Daten auf Basis eines Berechtigungskonzepts

3. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust:

- Backup-Strategie (online/offline; on-site/off-site)
- unterbrechungsfreie Stromversorgung (USV)
- Virenschutz
- Firewall
- Meldewege und Notfallpläne
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)
- Klimaanlage in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Erstellen eines Backup-Konzepts
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

4. Verfahren Zur Regelmässigen Überprüfung, Bewertung Und Evaluierung

Datenschutz-Management

- Festgelegte Verantwortlichkeiten für Datenschutz und Informationssicherheit
- Zertifiziertes Informationssicherheitsmanagementsystem gemäss ISO/IEC 27001
- Dokumentierte Datenschutz- und Informationssicherheitsrichtlinien
- Regelmässige Überprüfung und Aktualisierung der technischen und organisatorischen Massnahmen
- Regelmässige Sensibilisierung und Sicherheitsschulungen für Mitarbeitende
- Regelmässige Überprüfung von Zugriffsrechten und Berechtigungen
- Überprüfung und Überwachung von Auftragsverarbeitern und Unterauftragsverarbeitern, soweit anwendbar

Incident-Response-Management

- Dokumentierter Prozess zur Erkennung, Meldung und Behandlung von Sicherheitsvorfällen und Verletzungen des Schutzes personenbezogener Daten
- Interner Melde- und Eskalationsprozess für Sicherheitsvorfälle und Verletzungen des Schutzes personenbezogener Daten
- Einbindung des gruppeninternen Datenschutzbeauftragten und der Informationssicherheitsfunktionen bei Sicherheitsvorfällen und Verletzungen des Schutzes personenbezogener Daten, soweit anwendbar
- Dokumentation von Sicherheitsvorfällen und Verletzungen des Schutzes personenbezogener Daten über ein Ticketsystem
- Prozess zur Nachverfolgung von Sicherheitsvorfällen und Verletzungen des Schutzes personenbezogener Daten

Datenschutzfreundliche Voreinstellungen / Privacy By Design (Art. 25 Abs. 2 DS-GVO)

- Verfahren zur Sicherstellung datenschutzfreundlicher Voreinstellungen und der Berücksichtigung von Privacy-by-Design-Grundsätzen, soweit anwendbar

Auftragskontrolle

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers:

- Eindeutige Vertragsgestaltung
- formalisiertes Auftragsmanagement
- strenge Auswahl des Dienstleisters
- Vorüberzeugungspflicht
- Nachkontrollen

Anlage 2

Zusatzklauseln für die Bearbeitung von Personendaten, auf die das Bundesgesetz über den Datenschutz, Schweiz, Anwendung findet

- 1) "Personenbezogene Daten", "Verarbeitung", "Verantwortlicher", "Auftragsverarbeiter", "betroffene Person" und "Aufsichtsbehörde" haben die Bedeutung, die ihnen durch das schweizerische Bundesgesetz über den Datenschutz (Datenschutzgesetz) einschliesslich der einschlägigen Änderungen oder Revisionen und seiner Ausführungsverordnungen zugewiesen wird (wobei "die Behörde" die zuständige Datenschutzbehörde in dem Gebiet ist, in dem der Auftraggeber niedergelassen ist).
- 2) Die zuständige Aufsichtsbehörde für Datenbearbeitungen, auf die das Bundesgesetz über den Datenschutz Anwendung findet, ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) in der Schweiz.

Anlage 3

Unterauftragnehmer

Sofern im Einzelvertrag nichts anderes festgelegt ist, sind Unterauftragnehmer:

- 1) Compass Security Schweiz AG, Werkstrasse 20, 8640 Rapperswil-Jona, Schweiz
- 2) Compass Security Cyber Defense AG, Werkstrasse 20, 8640 Rapperswil-Jona, Schweiz
- 3) Compass Security Network Computing AG, Werkstrasse 20, 8640 Rapperswil-Jona, Schweiz

Die rechtlichen Verpflichtungen gelten für alle Unterauftragnehmer.

Kommunikation

Der Auftragnehmer verwendet Microsoft Software und die M365-Dienste des Anbieters Microsoft zur Bearbeitung von Daten und zur Kommunikation (MS Teams, MS Exchange Online, MS SharePoint, Microsoft 365 Copilot und mehr). Gemäss den aktuellen Einstellungen des Auftragnehmers und aktuellen Angaben von Microsoft werden Daten im Einklang mit den anwendbaren Zusagen von Microsoft zur Datenresidenz und, soweit konfiguriert und verfügbar, auf Servern in der Schweiz gespeichert. Angaben zu den Produkten und die darauf anwendbaren Bedingungen sind hier zu finden: <https://www.microsoft.com/licensing/terms/product/ForAllSoftware/all>

Mit der Nutzung von Microsoft Cloud-Produkten anerkennt der Auftraggeber die Microsoft-Nutzungsbedingungen sowie die Datenschutz- und Sicherheitsbestimmungen. Der Auftragnehmer weist darauf hin, dass die Microsoft-Bedingungen jederzeit ändern können. Die Microsoft Nutzungsbedingungen und Privacy Policy zum Schutz der Daten in der Microsoft Cloud finden sich hier: <https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/all> (Microsoft Privacy and Security Terms).

Ein umfassendes, dienstabhängiges Schutzkonzept stellt sicher, dass vertrauliche Kundendaten nicht mit Microsoft 365 Copilot bearbeitet werden. Insbesondere werden Kundendaten aus Mandaten und Projekten, einschliesslich Penetration Tests, Incident Response, digitaler Forensik, Analyse- oder Beratungsmandaten, nicht in Microsoft 365 Copilot eingegeben, hochgeladen oder anderweitig verarbeitet. Durch organisatorische und technische Massnahmen wird weiter sichergestellt, dass vertrauliche Kundendaten nicht unbeabsichtigt in die Microsoft Cloud gestellt werden. Das Schutzkonzept kann unter Beachtung der anwendbaren Vertraulichkeitsvereinbarungen bei Bedarf jederzeit eingesehen werden.

Server-Housing

Im Rahmen des Auftrages können Daten des Auftraggebers auf Servern gehostet werden, die sich im Rechenzentrum des Drittanbieters Green Datacenter AG (Industriestrasse 33, 5242 Lupfig, Schweiz) in der Schweiz befinden. Das Rechenzentrum ist ein Anbieter mit starkem Engagement für Datenschutz und -sicherheit. Es handelt sich um ein Server-Housing, bei dem das Rechenzentrum grundsätzlich keinen Zugriff auf die Daten hat.

Für Notfallsituationen, die ein physisches Eingreifen erfordern, hat der Auftragnehmer mit dem Rechenzentrum eine Remote-Hands-Vereinbarung getroffen, um Unterstützung vor Ort zu leisten. Ein solcher Zugriff ist streng auf nicht sensible betriebliche Aufgaben beschränkt und wird unter Anleitung des Auftragnehmers durchgeführt. Alle im Rahmen des Auftrages erhaltenen Daten werden sowohl bei der Übertragung als auch im Ruhezustand mit branchenüblichen Verschlüsselungsprotokollen verschlüsselt.

Der Auftragnehmer hat Verträge entsprechend den Datenschutzgesetzen abgeschlossen und stellt sicher, dass das Rechenzentrum strenge

Sicherheitsstandards erfüllt und die geltenden Datenschutzgesetze einhält, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten der Auftraggeber jederzeit zu gewährleisten.

Bug Bounty Programm

Sofern das Bug Bounty Programm Teil der vereinbarten Dienstleistungen ist, kann der Auftragnehmer freiberufliche Bug Hunter einsetzen, um Schwachstellen in den getesteten Assets des Auftraggebers zu identifizieren und zu melden. Diese Bug Hunter handeln innerhalb des Bug Bounty Programms unter angemessenen Vertraulichkeitsverpflichtungen. Im Rahmen dieser Tätigkeiten können freiberufliche Bug Hunter auf Daten einschliesslich Personendaten stossen. Aufgrund der Natur von Bug Bounty Aktivitäten und Bug Bounty Meldungen können Umfang und Kategorien der Personendaten, auf die zugegriffen oder die übermittelt werden könnten, nicht im Voraus bestimmt werden. Eine Übermittlung von Daten hat auf das zu beschränken, was zur Dokumentation und Bearbeitung der jeweiligen Schwachstellenmeldung erforderlich ist.

Der Auftragnehmer setzt Produkte von Atlassian (Atlassian Pty Ltd, Level 6, 341 George Street, Sydney NSW 2000, Australien) zur Kommunikation mit registrierten und nicht registrierten Nutzern sowie für Issue-Tracking und Dokumentation ein, insbesondere Atlassian Confluence und Jira Produkte. Personendaten unter dieser DVA werden Atlassian jedoch nur im Zusammenhang mit dem Bug Bounty Programm übermittelt, einschliesslich der Fälle, in denen Bug Hunter Daten, einschliesslich Personendaten, als Teil eines Bug-Reports hochladen. In diesem Zusammenhang kann eine Übermittlung von Daten in andere Länder, in denen Atlassian Dienstleistungen erbringt, einschliesslich der USA, nicht ausgeschlossen werden. Weitere Informationen zur Datenbearbeitung durch Atlassian finden sich hier: <https://www.atlassian.com/legal/privacy-policy>

Im Anwendungsfall des Bug Bounty Programms setzt der Auftragnehmer zusätzlich Hacking-Lab ein. Hacking-Lab wird von der OST (Ostschweizer Fachhochschule, Oberseestrasse 10, 8640 Rapperswil), einer öffentlichen Schweizer Hochschule mit starkem Hintergrund im Bereich Informationssicherheit, gehostet. Die OST fungiert als IaaS-Anbieterin, welche die Hacking-Lab-Infrastruktur betreibt, während die Hacking-Lab-Applikation selbst vom Auftragnehmer betrieben und gewartet wird.

Weitere Informationen zum Datenschutz der OST finden sich hier: <https://www.ost.ch/de/systemseiten/datenschutz>