Auftragsverarbeitungsvertrag (AVV) gemäß Art 28 Abs 3 DSGVO

Diese Vereinbarung bildet eine Ergänzung zu den AGB (nachfolgend "Hauptvertrag") und wird

zwischen

Kunde (nachfolgend "Verantwortlicher")

und

everbay GmbH (nachfolgend "Auftragsverarbeiter")

Schwanhildenweg 6
D-81673 München
Deutschland

(beide Parteien gemeinsam nachfolgend "Vertragsparteien")

geschlossen.

Mit dem Abschluss dieser Vereinbarung gehen die Vertragsparteien ein Auftragsverarbeitungsverhältnis ein. In dieser Vereinbarung gelten die entsprechenden Begriffsdefinitionen der DSGVO (Datenschutz-Grundverordnung - Verordnung (EU) 2016/679). Wenn daher in diesem Vertragswerk etwa der Begriff „Daten“ verwendet wird, dann sind damit „personenbezogene Daten“ im Sinne der DSGVO gemeint. Falls sich diese Vereinbarung und der Hauptvertrag bezüglich der Verarbeitung von personenbezogenen Daten widersprechen, geht diese Vereinbarung im Zweifel dem Hauptvertrag vor.

§ 1: Vertragsgegenstand und Dauer des Vertrages

1.1.: Dieser Vertrag findet Anwendung auf all jene Verarbeitungen personenbezogener Daten, die sich aus dem Hauptvertrag zwischen den Vertragsparteien ergeben, sofern der Auftragsverarbeiter diese personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet.

1.2.: Der Auftragsverarbeitungsvertrag tritt ab dem Zeitpunkt der Unterfertigung durch beide Parteien in Kraft. Er gilt akzessorisch zum Hauptvertrag und bleibt jedenfalls für die Dauer der datenschutzrechtlich relevanten Leistungserbringung aus dem Hauptvertrag in Geltung. Bei vollständigem Wegfall des Hauptvertrages erlischt auch diese Vereinbarung automatisch. Es bedarf in diesem Fall keiner gesonderten Kündigung.

1.3.: Dieser Vertrag und somit das gesamte Auftragsverarbeitungsverhältnis kann von den Vertragsparteien zu jeder Zeit ohne Einhaltung einer Frist aufgekündigt werden, wenn die jeweils andere Partei schwerwiegend gegen

diese Vereinbarung oder das einschlägige Datenschutzrecht verstößt.

Solch ein schwerwiegender Verstoß ist etwa dann gegeben, wenn der Auftragsverarbeiter die Pflichten, die sich aus dieser Vereinbarung und aus dem Art 28 DSGVO ergeben, nicht einhält. Weiters kann der Verantwortliche fristlos kündigen, wenn der Auftragsverarbeiter eine Weisung des Verantwortlichen nicht befolgt, wenn der Auftragsverarbeiter die vertragsmäßig festgelegten Kontrollrechte des Verantwortlichen verweigert oder wenn der Auftragsverarbeiter zwingend notwendige oder vereinbarte Sicherheitsmaßnahmen unterlässt.

§ 2: Art und Zweck der Verarbeitung

2.1.: Die personenbezogenen Daten verarbeitet der Auftragsverarbeiter ausschließlich zur Erfüllung seiner vertraglichen Pflichten aus dem Hauptvertrag.Die Verarbeitung erfolgt daher aufgrund des Hauptvertrages, dieser Vereinbarung oder gemäß einer Weisung des Verantwortlichen. Dem Auftragsverarbeiter ist es untersagt personenbezogene Daten für eigene oder fremde Zwecke zu verarbeiten oder personenbezogene Daten, ohne vorherige schriftliche Weisung des Verantwortlichen an Dritte weiterzugeben. Die Duplizierung oder Kopie von personenbezogenen Daten durch den Auftragsverarbeiter ist nur so weit erlaubt, als diese im Vorhinein durch den Verantwortlichen genehmigt wurde oder diese für die Sicherstellung der ordnungsgemäßen Datenverarbeitung (Kopie zur Sicherung) oder zur Einhaltung gesetzlicher Pflichten (zB gesetzliche Aufbewahrungspflichten) unbedingt notwendig ist.

2.2.: Die konkreten Verarbeitungsarten (Art 4 Z 2 DSGVO) und Zwecke der Verarbeitung des Auftragsverarbeiters sind dem Hauptvertrag zu entnehmen.

§ 3: Art der personenbezogenen Daten, Kategorien betroffener Personen

Die durch den Auftragsverarbeiter verarbeiteten Arten personenbezogener Daten sowie die Kategorien der betroffenen Personen finden sich in Anhang 1. Der Anhang 1 stellt einen Teil dieser Vereinbarung dar.

§ 4: Rechte und Pflichten des Verantwortlichen

4.1.: Dem Verantwortlichen obliegt allein die Entscheidung über die Mittel und Zwecke der Verarbeitung von den von ihm zur Verfügung gestellten personenbezogenen Daten.

4.2.: Der Verantwortliche verpflichtet sich die EU-rechtlichen und nationalen Datenschutzbestimmungen sowie diese Vereinbarung einzuhalten. Er ist insbesondere dafür verantwortlich, die Rechtmäßigkeit der Verarbeitung personenbezogener Daten (Art 6 DSGVO) zu beurteilen und dass die Rechte der betroffenen Personen gemäß den Art 12 – 22 DSGVO gewahrt werden. Gleichzeitig obliegt die Entscheidung über die Beantwortung einer Anfrage einer betroffenen Person bezüglich ihrer Betroffenenrechte ausschließlich dem Verantwortlichen und die entsprechende Kommunikation erfolgt nur durch diesen.

4.3.: Der Verantwortliche ist berechtigt dem Auftragsverarbeiter Weisungen und Aufträge bezüglich Art und Umfang der Verarbeitung personenbezogener Daten zu erteilen.

Diese Aufträge und Weisungen sind durch den Verantwortlichen grundsätzlich auf eine dokumentierte und schriftliche oder elektronische Weise zu erteilen. Wenn Weisungen mündlich erteilt werden, sind diese schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Unter einer Weisung versteht dieses Vertragswerk eine Anordnung an den Auftragsverarbeiter bezüglich des Umgangs mit personenbezogenen Daten.

4.4.: Datenträger oder Datensätze, die der Verantwortliche dem Auftragsverarbeiter überlässt, verbleiben im Eigentum des Verantwortlichen. Der Verantwortliche ist jederzeit berechtigt dem Auftragsverarbeiter die Löschung, Berichtigung, Herausgabe, Anpassung oder Einschränkung der Datenverarbeitung anzuordnen.

4.5.: Der Verantwortliche meldet dem Auftragsverarbeiter unverzüglich Fehler und Auffälligkeiten, die ihm an Ergebnissen der Auftragsverarbeitung auffallen.

4.6.: Der Verantwortliche ist verpflichtet den Auftragsverarbeiter unverzüglich zu verständigen, wenn es zu einem Wechsel des Datenschutzbeauftragten kommt.

§ 5: Pflichten des Auftragsverarbeiters

5.1.: Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur aufgrund der dokumentierten Weisung des Verantwortlichen, sofern der Auftragsverarbeiter nicht durch das Recht der Union oder der Mitgliedstaaten hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

5.2.: Der Auftragsverarbeiter ist verpflichtet personenbezogene Daten zu löschen, zu berichtigen, herauszugeben, anzupassen oder einzuschränken, wenn dies vom Verantwortlichen angeordnet wird.

5.3.: Der Auftragsverarbeiter hat zu gewährleisten, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

5.4.: Der Auftragsverarbeiter verpflichtet sich alle technischen und organisatorischen Maßnahmen (TOMs) im Sinne des Art 32 DSGVO, die für die Sicherheit der Verarbeitung von personenbezogenen Daten erforderlich sind, zu ergreifen. Die durch den Auftragsverarbeiter gesetzten TOMs sind im Anhang 2 näher beschrieben. Der Anhang 2 stellt einen Teil dieser Vereinbarung dar.

5.5.: Der Verantwortliche erklärt sich mit den im Anhang 3 gelisteten weiteren Auftragsverarbeitern (nachfolgend „Sub-Auftragsverarbeiter) einverstanden. Diese gelisteten Sub-Auftragsverarbeiter sind zur Erfüllung des Hauptvertrages erforderlich. Ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung nimmt der Auftragsverarbeiter keine weiteren Auftragsverarbeiter in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung ist der Auftragsverarbeiter verpflichtet, den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Sub-Auftragsverarbeiter zu informieren. Der Verantwortliche hat dann die Möglichkeit gegen die Änderung innerhalb einer angemessenen Frist Einspruch zu erheben.

5.6.: Mit beauftragten Sub-Auftragsverarbeitern wird durch den Auftragsverarbeiter eine vertragliche Vereinbarung geschlossen, die zumindest das gleiche Datenschutzniveau wie dieser Vertrag zwischen dem Verantwortlichen und Auftragsverarbeiter gewährleistet. Dabei werden alle gesetzlichen und vertraglichen Vorgaben berücksichtigt, insbesondere die technischen und organisatorischen Maßnahmen gemäß Art 32 DSGVO.

5.7.: Verstößt ein Sub-Auftragsverarbeiter gegen seine datenschutzrechtlichen Pflichten, haftet der Auftragsverarbeiter dem Verantwortlichen für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters. Der Verantwortliche kann im Falle eines Verstoßes gegen datenschutzrechtliche Pflichten durch den Sub-

Auftragsverarbeiter den Auftragsverarbeiter anweisen die Beschäftigung des Sub-Auftragsverarbeiters ganz oder teilweise zu beenden.

5.8.: Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit, damit dieser die Rechte der betroffenen Person nach Kapitel III der DSGVO innerhalb der gesetzlichen Fristen erfüllen kann. Dafür ergreift der Auftragsverarbeiter technische und organisatorische Maßnahmen. Wird ein Antrag irrtümlicherweise an den Auftragsverarbeiter gestellt und ist es ersichtlich, dass er eigentlich an den Verantwortlichen gestellt werden hätte sollen, so leitet der Auftragsverarbeiter den Antrag unverzüglich an den Verantwortlichen weiter und benachrichtigt diesen auch.

5.9.: Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung der in Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgenabschätzung, vorherige Konsultation der Aufsichtsbehörde).

5.10.: Der Auftragsverarbeiter verpflichtet sich nach Erbringung der Verarbeitungsleistungen oder davor nach Anordnung des Verantwortlichen, spätestens mit Beendigung des Hauptvertrages alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben und vorhandene Kopien zu löschen.

Der Auftragsverarbeiter ist berechtigt Dokumentationen, unter Berücksichtigung der einschlägigen Aufbewahrungsfristen, für den Nachweis der auftrags- und ordnungsgemäßen Datenvereinbarung auch nach Beendigung des Vertragsverhältnisses aufzubewahren.

5.11.: Der Auftragsverarbeiter erklärt sich damit einverstanden, dass der Verantwortliche selbst oder durch Dritte Überprüfungen und Inspektionen bezüglich der Einhaltung der Vorschriften über Datenschutz und Datensicherheit beim Auftragsverarbeiter durchführt. Der Auftragsverarbeiter stellt alle dafür erforderlichen Informationen zur Verfügung und wirkt unterstützend mit. Der Verantwortliche hat für diese Überprüfungen und Inspektionen grundsätzlich einen Termin zu vereinbaren. Der Verantwortliche darf seine Kontrollrechte nur in einem angemessenen und erforderlichen Umfang ausüben.

5.12.: Der Auftragsverarbeiter informiert den Verantwortlichen umgehend, wenn es zu schwerwiegenden Störungen des Betriebsablaufes kommt, wenn er der Ansicht ist, dass eine Weisung gegen gesetzliche Datenschutzbestimmungen verstößt, es zu Verstößen durch Mitarbeiter oder Sub-Auftragsverarbeiter kommt oder wenn sich Unregelmäßigkeiten im Zuge der Verarbeitung der Daten des Verantwortlichen ergeben. Der Auftragsverarbeiter kann die Durchführung von Weisungen, die gegen gesetzliche Datenschutzbestimmungen verstoßen, aussetzen, bis sie durch den Verantwortlichen bestätigt oder abgeändert wurden.

§ 6: Vertraulichkeit

Die Vertragsparteien verpflichten sich, alle Kenntnisse von betriebsinternen Geheimnissen oder datenschutzrechtlicher Sicherheitsmaßnahmen der jeweils anderen Vertragspartei vertraulich zu behandeln und nicht an Dritte weiterzugeben. Diese Verpflichtung gilt auch nach Beendigung des Vertrages weiterhin.

§ 7: Schriftlichkeit bei Änderungen

Jegliche Änderungen oder Ergänzungen dieser Vereinbarung bedürfen für Ihre Wirksamkeit der Schriftform. Dies gilt auch für Änderungen dieser Schriftformklausel.

§ 8: Haftung

Etwaige im Hauptvertrag geregelten Haftungsprivilegierungen finden auf diese Vereinbarung keine Anwendung. Für nachteilige Folgen von Verletzungen datenschutzrechtlicher Pflichten im Rahmen des vertraglich und gesetzlich bestimmten eigenen Verantwortungsbereichs haftet jede Vertragspartei im Innenverhältnis allein und uneingeschränkt. In diesem Zusammenhang verpflichten sich sowohl der Verantwortliche als auch der Auftragsverarbeiter den jeweils anderen bei einer Inanspruchnahme durch Dritte vollumfänglich schad- und klaglos zu halten.

Davon sind insbesondere auch behördliche Geldbußen umfasst, die über eine Vertragspartei aufgrund des der anderen Vertragspartei zuzurechnenden Verhaltens verhängt wurden.

§ 9: Rechtswahl und Gerichtsstand

Diese Vereinbarung unterliegt deutschem Recht sowie dem sachlich relevanten Unionsrecht, insbesondere der DSGVO. Ausschließlicher Gerichtsstand ist der Sitz des Auftragsverarbeiters.

§ 10: Salvatorische Klausel

Sollten einzelne Bestimmungen dieses Vertrages undurchführbar oder unwirksam sein, wird die Wirksamkeit der übrigen Bestimmungen davon nicht berührt.

Anhang 1: Datenverarbeitungsspezifikationen

Begriffserklärungen zu Datenkategorien

	Beschreibung zur Datenkategorie
Keine personenbezogenen Daten	
Bildaufzeichnungen	Filme, Fotografien, Videoaufzeichnungen, digitale Fotos.
Berufliche Tätigkeiten	Art der von der betroffenen Person genutzten bzw. gelieferten Tätigkeiten, Güter oder Dienstleistungen, Geschäftskontakte.
Berufserfahrung	Berufliche Interessen, Forschungsinteressen, Studieninteressen, Spezialisierungsthemen, Unterrichtserfahrungen, Beratungen.
Schulische Laufbahn	Chronologie der besuchten Schulen, Einrichtungen, Universitäten, Art der besuchten Kurse, bestandene Diplome, Prüfungsergebnisse, andere erhaltene Diplome, Beurteilungen des Studienfortschritts.
Berufsqualifikation	Berufliche Abschlüsse und Ausbildungen, spezielle Lizenzen (Piloten, ...).
Persönliche Identifikationsdaten	Name, Titel, (private und berufliche) Adresse, frühere Adressen, (private, berufliche) Telefonnummer, von der für die Verarbeitung verantwortliche Person zugeteilte Kennnummern.
Persönliche Detailangaben	Alter, Geschlecht, Geburtsdatum, Geburtsort, Familienstand und Nationalität.

Bereich: Social Recruiting

Verarbeitung	02.01 Schalten von Stellenanzeigen auf Social Media
Zweck der Verarbeitung	Wir Schalten Stellenanzeigen auf Sozialen Netzwerken um Bewerber für unsere Kunden zu generieren. Über die Stellenanzeigen werden die potentiellen Bewerber auf einen Funnel weitergeleitet. Auf den sozialen Netzwerken können wir nicht einsehen welche konkreten Personen auf unsere Werbeanzeigen geklickt haben. Es findet daher keine Verarbeitung personenbezogener Daten statt.
Datenkategorie	• Keine personenbezogenen Daten
Personengruppe	• Social Media Nutzer
Empfänger	-

Verarbeitung	02.02 Erhebung und Speicherung von Bewerberdaten
Zweck der Verarbeitung	Bewerber die durch eine Stellenanzeige von Social Media weitergeleitet wurden, haben die Möglichkeit die für die ausgeschriebene Stelle erforderlichen Daten anzugeben. Dies sind klassische Bewerberdaten wie etwa Sprachkenntnisse oder Qualifikationen. Je nach Ausschreibung kann auch ein Lebenslauf hochgeladen werden. Diese Daten werden in der Software Perspective gespeichert. Für die Auswahl geeigneter Personen wird ein Profiling-Verfahren verwendet. Dabei werden die personenbezogene Daten automatisiert verarbeitet und die angegebenen Informationen bewertet und analysiert.
Datenkategorie	• Bildaufzeichnungen • Berufliche Tätigkeiten • Berufserfahrung • Schulische Laufbahn • Berufsqualifikation • Persönliche Identifikationsdaten • Persönliche Detailangaben
Personengruppe	• Bewerber (Social Recruiting)
Empfänger	• Perspective

Verarbeitung	02.03 Übermittlung der Bewerberdaten an den Auftraggeber
Zweck der Verarbeitung	Die erhobenen Daten werden dann über die Sendinblue GmbH an den Auftraggeber übermittelt damit dieser Kontakt mit dem Bewerber aufnehmen kann.
Datenkategorie	• Bildaufzeichnungen • Berufliche Tätigkeiten • Berufserfahrung • Schulische Laufbahn • Berufsqualifikation • Persönliche Identifikationsdaten • Persönliche Detailangaben
Personengruppe	• Bewerber (Social Recruiting)
Empfänger	• Sendinblue GmbH

Verarbeitung	02.04 16.04 Übertragung der Daten in ein digitales Kanban-Board
Zweck der Verarbeitung	Alternativ zur Übermittlung der Bewerberdaten per Mail werden erstellte Bewerbungsprofile in ein digitales Kanban-Board überspielt. Dadurch ist ein besseres Management der Bewerbungen möglich. Das verwendete Tool ist Meistertask von Meister Labs GmbH. Dadurch können Bewerbungen besser organisiert und verwaltet werden.
Datenkategorie	• Bildaufzeichnungen • Berufliche Tätigkeiten • Berufserfahrung • Schulische Laufbahn • Berufsqualifikation • Persönliche Identifikationsdaten • Persönliche Detailangaben
Personengruppe	• Bewerber (Social Recruiting)
Empfänger	• MeisterLabs GmbH

Verarbeitung	02.05 Kontaktierung
Zweck der Verarbeitung	Die Bewerber werden mit den von Ihnen zur Verfügung gestellten Möglichkeiten kontaktiert. Dies kann beispielsweise per Mail, SMS, Anruf oder durch eine Nachricht über einen Messenger erfolgen
Datenkategorie	• Persönliche Identifikationsdaten
Personengruppe	• Bewerber (Social Recruiting)
Empfänger	-

Anhang 2: Technisch organisatorische Maßnahmen (Art 32 Abs 1 DSGVO)

Schutzart: 1.1.1 Vertraulichkeit: Zutrittskontrolle
1.1.1.03 Zugängliche Fenster und Außentüren der Unternehmensräumlichkeiten sind einbruchssicher ausgeführt
1.1.1.04 Eingangstüren zu Unternehmensgebäuden oder Räumen sind durch eine genormte Schließanlage gesichert (Sicherheitsschlösser, Chipkarten, Transponder, Codeschloss)
1.1.1.05 Eingangstüren zu Unternehmensräumlichkeiten weisen neben Schließanlagen, zusätzliche Zutrittssicherungen auf (zb. Türknauf außen)
1.1.1.06 Die Vergabe, Verlust und Rückgabe von Schlüsseln, Transpondern, Chipkarten oder Codes an Personen wird dokumentiert
1.1.1.08 Es ist sichergestellt, dass Personen nur dort Zutritt erhalten, wo Sie für die Erfüllung Ihrer Aufgaben auch Zutritt benötigen

Schutzart: 1.1.2 Vertraulichkeit: Zutrittskontrolle (sensible Räume)
1.1.2.05 Bildschirme auf denen Personaldaten verarbeitet werden sind von außen (Fenster) oder innen (Glastüre oder Glasfront) nicht einsehbar
1.1.2.10 Bildschirme auf denen sensible Kundendaten verarbeitet werden sind von außen (Fenster) oder innen (Glastüre oder Glasfront) nicht einsehbar
1.1.2.15 In sensiblen Räumlichkeiten (Personal, Kundenverwaltung, IT) befinden sich keine Geräte, zu denen ein Benutzerkreis außerhalb der eigentlich Berechtigten Zugang benötigt (zB. Drucker)

Schutzart: 1.2 Vertraulichkeit: Zugangskontrolle

1.2.02 Laptops oder Smart Devices (Ipad etc.) werden nach Dienstende versperrt aufbewahrt oder werden mit nach Hause genommen

1.2.04 Das Bios von Clients ist mit einem gesonderten Passwort gesichert

1.2.07 Sammelaccounts oder unpersonalisierte Benutzerzugänge auf Clients (mehrere Benutzer teilen sich einen Zugang) existieren nicht

1.2.08 Auf jedem verwendeten Client (Rechner) ist eine Firewall aktiv

1.2.09 Auf jedem Client Rechner ist eine Antiviren Software installiert, diese wird täglich bzw. bei einer Neuanmeldung aktualisiert

1.2.10 Eingehende Mails werden online am E-Mail Server (beim Hoster) auf Viren geprüft

1.2.11 Eingehende Mails werden online am Mail Server (Hoster) auf Spam geprüft

1.2.12 Auf jedem Client Rechner ist eine (Antiviren) Software installiert die beim Surfen im Internet entsprechenden Schutz (Webfilter) bietet

1.2.13 Bei Routern ins Internet (WLAN Router) sind nur die absolut erforderlichen Ports freigeschaltet

1.2.14 Der Zugang zum internen Netzwerk (WLAN) ist mit einem eigenen Passwort gesichert

1.2.16 Der Zugang zur Konfigurationsoberfläche des (WLAN) Routers wurde mit einem eigenen Benutzernamen und einem eigenen Passwort (ungleich Standard Benutzeraccount) gesichert

1.2.19 Eine Firewall ist auf jedem Übergang zum Internet aktiviert (Router)

1.2.20 Wir setzen Systeme ein, die Zugriffsversuche oder Angriffe von betriebsfremden Personen identifizieren und/ oder verhindern können (inrusion detection System)

1.2.21 Auf jedem Server und sonstigen Systemen bei denen ein Datenaustausch über das Internet erfolgt ist eine Antiviren Software installiert die täglich aktualisiert wird

1.2.22 Mobile Endgeräte werden durch den Einsatz einer Antiviren Software geschützt

1.2.24 Bei Bildschirmen die in Räumlichkeiten eingesetzt werden, zu denen Kunden (Patienten...) Zugang haben und personenbezogene Daten verarbeitet werden, wird darauf geachtet, dass der Bildschirm nicht eingesehen werden kann. Allenfalls existiert ein entsprechender Sichtschutz.

1.2.25 Bildschirme werden automatisch bei Inaktivität gesperrt und können nur durch Eingabe des Benutzerpasswortes oder ähnliche Verfahren (Fingerprint, Gesichtserkennung, etc.) wieder entsperrt werden

Schutzart: 1.3 Vertraulichkeit: Zugriffskontrolle

1.3.01 Die Anzahl der Administratoren für Server und zentrale Software ist auf das „Notwendigste“ reduziert

1.3.02 Jeder Administrator verfügt über einen eigenen Benutzeraccount und das Passwort besteht zumindest aus 12 Stellen

1.3.04 Passwörter müssen so gewählt werden, dass sie sich von den letzten Passwörtern (zb. letzten 6 verwendeten) unterscheiden müssen

1.3.05 Passwörter von Benutzern weisen eine ausreichende Komplexität auf (beinhalten Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern und weisen eine Mindestlänge von 8 Stellen auf)

1.3.06 Die Verwaltung von Benutzerrechten für genutzte Software erfolgt zentral über festgelegte Systemadministratoren

1.3.07 Jeder Benutzer erhält für jedes System und jede Software die er für seine Tätigkeit benötigt einen eigenen Benutzeraccount (keine Sammelaccounts)

1.3.08 Jeder Benutzer erhält auf Basis des "need to know" Prinzip, nur die Zugriffsrechte (auf Daten, Systeme, Software, Dateiablagesysteme) die er für seine Tätigkeit auch zwingend benötigt

1.3.09 Beim Ausscheiden eines Benutzers aus dem Unternehmen ist sichergestellt, dass seine Zugriffsberechtigungen umgehend entfernt und der Benutzer nach Ablauf einer gewissen Frist auch gelöscht wird.

1.3.10 Die Vergabe von Zugriffsberechtigungen erfolgt auf Basis von definierten Benutzerprofilen

1.3.11 Fällt die Notwendigkeit eines oder mehrerer Zugriffsrechte bei einem Benutzer weg, dann werden ihm die Rechte auch zeitnah entzogen

1.3.12 Zugriffe auf sensible Anwendungen oder Daten werden protokolliert (wer hat wann auf Daten zugegriffen, sie verändert oder gelöscht)

1.3.13 Papierakten mit personenbezogenen Daten werden durch den Einsatz von Aktenshredder mind. Stufe 3, Cross-cut geshreddert

1.3.14 Elektronische Datenträger werden datenschutzkonform gemäß der Sicherheitsstufe F-4, O-4, T-4, H-4, E-4 vernichtet

Schutzart: 1.4 Vertraulichkeit: Trennungsgebot

1.4.01 Daten die im Rahmen einer Auftragsverarbeitung elektronisch verarbeitet werden, liegt eine Trennung in Mandanten vor. Es ist gewährleistet, dass die Daten eines Mandanten vor dem Zugriff durch andere Mandanten geschützt ist.

1.4.02 Bei Softwareapplikationen die personenbezogene Daten verarbeitet existiert eine Trennung in Test- und Produktivsystem

1.4.03 Der Zugriff auf Daten in Datenbanken ist geregelt

1.4.04 Die Sicherung der Daten (Backup) erfolgt auf physisch und örtlich getrennte Medien

1.4.05 Softwareapplikationen und Dateiablagen auf die mehrere Benutzer Zugriff haben, sind mit einem Berechtigungssystem ausgestattet.

1.4.06 Die Verarbeitung von personenbezogenen Daten erfolgt nur zu den festgelegten Zwecken

1.4.07 Die Weitergabe von personenbezogenen Daten erfolgt nur zu den festgelegten Zwecken

Schutzart: 1.6 Vertraulichkeit: Verschlüsselung

1.6.02 Festplatten in Laptops / Notebooks werden verschlüsselt

1.6.04 Zur Datenweitergabe werden verschlüsselte Verbindungen wie https (Webseite) oder sftp (FTP Server) genutzt

1.6.06 Es wird die aktuellste Version des TLS Verschlüsselungsprotokolls verwendet

1.6.07 Die Versendung von Mails mit sensiblem Inhalt oder sensiblen Daten im Mail oder in Anhängen erfolgt verschlüsselt

1.6.08 Datenbanken in den personenbezogene Daten verarbeitet werden sind verschlüsselt

Schutzart: 2.1 Integrität: 1. Eingabekontrolle

2.1.01 Dokumente oder Formulare in denen sensible Daten erhoben werden, werden aufbewahrt sofern diese automatisch weiterverarbeitet werden, um Datenfehlübernahmen korrigieren zu können.

2.1.02 Es existiert eine Übersicht/ Dokumentation, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.

2.1.03 Die Eingabe, Änderung und Löschung von Daten durch individuelle Benutzer (nicht Benutzergruppen) kann nachvollzogen werden

2.1.04 Es erfolgt eine technische Protokollierung der Eingabe, Änderung und Löschung von Daten inkl. Zeitpunkt der Änderung und wer die Daten geändert hat

2.1.05 Die An- und Abmeldung an Softwareapplikationen auf die mehrere Benutzer Zugriff haben wird protokolliert

2.1.06 Die An- und Abmeldung auf Servern wird protokolliert

Schutzart: 2.2. Integrität: 2. Weitergabekontrolle

2.2.01 Die Übermittlung von personenbezogenen Daten zu Lieferanten (Auftragsverarbeiter) erfolgt verschlüsselt (Mailverschlüsselung, VPN Tunnel etc.)

2.2.03 Auf Rechner wird mittels Fernwartung nur nach Zustimmung des Benutzers zugegriffen. Ausgenommen davon sind Update und Konfigurationsvorgänge am Rechner mit Hilfe automatischer Installationstools.

2.2.04 Die Datenträger von Laptops oder Desktops werden vor deren internen oder externen Weitergabe gelöscht, formatiert oder physisch zerstört

2.2.05 Sonstige Datenträger (USB Sticks, mobile Festplatten, ausgebaute Festplatten) werden vor deren internen oder externen Weitergabe gelöscht, formatiert oder physisch zerstört

2.2.06 Bei Druckern oder Faxgeräten werden deren interne Datenträger vor der externen Weitergabe gelöscht, formatiert, physisch zerstört oder nach Vorgaben des Herstellers gelöscht

2.2.07 Die Weitergabe von personenbezogenen Daten an Dritte erfolgt in anonymisierter oder pseudonymisierter Form

2.2.08 Für die Aktenvernichtung werden Dienstleister (nach Möglichkeit mit Datenschutz-Gütesiegel) eingesetzt

Schutzart: 3.1 Verfügbarkeit und Belastbarkeit: Verfügbarkeitskontrolle
3.1.01 Auf Clients und Servern werden Updates und Sicherheitspatches regelmäßig eingespielt
3.1.02 Von relevanten Systemen (zB. Buchhaltung, CRM, HR Software) oder sonstigen Systemen die personenbezogene Daten verarbeitet werden, werden regelmäßige Datensicherungen erstellt
3.1.03 Datensicherungen werden räumlich getrennt von den Produktivdaten aufbewahrt
3.1.04 Es wird regelmäßig geprüft ob Datensicherungen vollständig rückgesichert werden können und Daten damit wieder hergestellt werden können
3.1.05 Datensicherungen werden nach einem definierten Zeitraum gelöscht
3.1.06 Räumlichkeiten in denen personenbezogene Daten verarbeitet werden, sind mit einer Feuer- und Rauchmeldeanlage ausgestattet
3.1.07 Räumlichkeiten in denen personenbezogene Daten verarbeitet werden, verfügen leicht erreichbar, über geeignete Löschmittel zur Brandbekämpfung (zB. Feuerlöscher)

Schutzart: 4.1 Verfahren zur Überprüfung: Datenschutz-Management
4.1.01 Es wurde ein interner oder externer Datenschutz Beauftragter bestellt
4.1.02 Es wird ein Verzeichnis der Verarbeitungstätigkeiten geführt und laufend aktualisiert
4.1.03 Eine Audit/ Überprüfung der Wirksamkeit der technisch organisatorischen Maßnahmen findet jährlich statt
4.1.04 Es existieren Abläufe zur Erfüllung der Rechte von betroffenen Personen
4.1.05 Eine Datenschutz Management Software ist im Einsatz
4.1.06 Die Informationspflichten (Datenschutzerklärung) werden regelmäßig geprüft
4.1.07 Es existiert ein Löschkonzept in dem festgelegt ist, wann, welche Daten zu löschen sind. Die Löschung von Daten wird stichprobenartig oder regelmäßig überprüft.
4.1.10 Alle Mitarbeiter sind auf Vertraulichkeit und Datengeheimnis verpflichtet
4.1.11 Mitarbeiter werden jährlich im Bereich Datenschutz geschult bzw. nachweislich sensibilisiert
4.1.12 Alle Mitarbeiter sind nachweislich geschult, wie sie bei Anfragen von Betroffenen zu Auskunft oder Löschung der Daten vorgehen sollen
4.1.14 Eine Richtlinie zur richtigen Verwendung und Aktualisierung von Passwörtern wurde erstellt und die Mitarbeiter werden dahingehend geschult
4.1.15 in Bereichen in denen sensible personenbezogene Daten verarbeitet werden existiert eine Clean/ Clear Desk Richtlinie. Die betroffenen Mitarbeiter werden regelmäßig dahingehend sensibilisiert.
4.1.16 Eine Clear Screen Richtlinie ist definiert und die Mitarbeiter werden regelmäßig sensibilisiert
4.1.17 Eine Closed door Richtlinie für kritische/ sensible Bereiche (zb. Personalbüro, IT) ist definiert und wird im Unternehmen aktiv gelebt
4.1.18 Eine Mobil Device Richtlinie wurde definiert und deren Einhaltung wird regelmäßig überprüft
4.1.20 Mitarbeiter sind angewiesen, die gültigen Datenschutzmaßnahmen auch im Home Office zu gewährleisten
4.1.21 Um bei Angriffen auf die IT oder Katastrophenfällen geordnet reagieren zu können, haben wir einen Notfallplan erstellt.

Schutzart: 4.2 Verfahren zur Überprüfung: Incident-Response-Management

4.2.01 Fehlerhafte Login Versuche führen zu einer automatischen Sperre des Benutzer Logins. Die Sperre bleibt für einen definierten Zeitraum (siehe Passwort Richtlinie) bestehen.

4.2.02 Ein Ablauf zur Meldung von Sicherheitsverletzungen an die Datenschutz Behörde und betroffene Personen existiert

4.2.07 Verarbeitungen werden hinsichtlich einer Datenschutz Folgeabschätzung geprüft. Eine solche wird bei Bedarf auch durchgeführt und dokumentiert

4.2.08 Ein IT Security Manager ist bestellt

Schutzart: 4.4 Verfahren zur Überprüfung: Auftragskontrolle

4.4.01 Es existiert eine Übersicht über alle Lieferanten (Empfänger), die in unserem Namen personenbezogene Daten als Auftragsverarbeiter verarbeiten

4.4.02 Die Auswahl des Auftragnehmers erfolgt unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

4.4.03 Wir beauftragen nur Unternehmen mit der Verarbeitung von personenbezogenen Daten, nur wenn sie einen Datenschutzbeauftragten bestellt haben

4.4.04 Mit all unseren Auftragsverarbeitern haben wir einen Auftragsverarbeitervertrag abgeschlossen

4.4.05 Es sind wirksame Kontrollrechte gegenüber dem Auftragnehmern vertraglich (Auftragsverarbeitervertrag) vereinbart

4.4.06 In den Auftragsverarbeiter Verträgen ist sicher gestellt, dass Daten nach Beendigung des Auftrags auch vernichtet oder übergeben werden

4.4.07 Wir überprüfen regelmäßig ob unsere Auftragsverarbeiter die festgelegten Datenschutzmaßnahmen einhalten

4.4.08 Die Wirksamkeit von Datenschutzmaßnahmen oder die Gültigkeit entsprechender Zertifikate werden bei Auftragsverarbeitern regelmäßig geprüft

4.4.10 Mitarbeiter von Auftragnehmern werden auf das Datengeheimnis verpflichtet bzw. der Auftragnehmer muss dies seinerseits sicher stellen

Anhang 3: Subunternehmen (weitere Auftragsverarbeiter)

Bezeichnung	Land	Übermittlung Drittland
Perspective	Deutschland	EU
Sendinblue GmbH	Deutschland	EU
MeisterLabs GmbH	Deutschland	EU