Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen

dem Unternehmen, dass sich durch die Registrierung unter https://www.viguard.eu/register ein Kundenkonto anlegt.

Auftraggeber,

und

blackpoint GmbH

Friedberger Str. 106b
61118 Bad Vilbel

Ansprechpartner: Dirk Estenfeld

Auftragnehmer.

§1
Anwendungsbereich

Die Vereinbarung findet Anwendung auf alle Tätigkeiten, die Gegenstand der zwischen den Parteien geschlossenen Vereinbarung („Leistungsvereinbarung“) sind und bei deren Verrichtung Mitarbeiter des Auftragsnehmers oder durch den Auftragnehmer nach Maßgabe dieser Vereinbarung beauftragte Dritte mit personenbezogenen Daten in Berührung kommen, für die der Auftraggeber gemäß Art. 4 Nr. 7 DS-GVO Verantwortlicher ist.

§2
Begriffsbestimmung

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers i. S. v. Art. 28 DS-GVO (Auftragsverarbeitung). Der Auftraggeber bleibt im datenschutzrechtlichen Sinn Verantwortlicher („Herr der Daten“).

Der Auftragnehmer darf die personenbezogenen Daten im Rahmen des datenschutzrechtlich Zulässigen für eigene Zwecke auf eigene Verantwortung verarbeiten, wenn eine gesetzliche Erlaubnisvorschrift oder eine Einwilligungserklärung der betroffenen Person das gestattet. Auf solche Datenverarbeitungen findet dieser Vertrag keine Anwendung. In jedem Fall darf der Auftragnehmer die personenbezogenen Daten anonymisieren und in anonymisierter Form für eigene Zwecke verarbeiten und nutzen, insbesondere für statistische Zwecke.

§3
Konkretisierung des Auftragsinhalts, Laufzeit und Kündigung

Die Verarbeitung der „Auftraggeber-Daten“ im Rahmen der Auftragsverarbeitung erfolgt entsprechend den in **Anlage 1** zu diesem Vertrag enthaltenen Festlegungen zu Art, Umfang und Zweck der Datenverarbeitung. Sie bezieht sich auf die in **Anlage 1** festgelegte Art der „Auftraggeber-Daten“ und die dort bestimmten Kategorien betroffener Personen.

Die Dauer des Auftrags richtet sich nach der Laufzeit des Hauptvertrags. Die Vereinbarung bleibt so lange anwendbar, bis alle Daten wieder an den Auftraggeber zurückgegeben oder gelöscht wurden.

§4
Verantwortlichkeit und Weisungsbefugnis

Der Auftraggeber ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (Art. 4 Nr. 7 DS-GVO). Er kann jederzeit die Herausgabe, Berichtigung, Löschung und Einschränkung der Daten bzw. deren Verarbeitung verlangen. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung im Auftrag Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen, wenn und soweit den Auftragnehmer nicht gemäß Art. 82 DS-GVO eine eigene Haftung trifft.

Auskünfte an Dritte oder betroffene Personen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen. Soweit eine betroffene Person sich zwecks Ausübung der ihr nach Artt. 15 ff. DS-GVO zukommenden Rechte unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Für den Fall, dass eine betroffene Person die ihr nach den Artt. 15 ff. DS-GVO zukommenden Rechte geltend macht, hat der Auftragnehmer den Auftraggeber bei der Erfüllung dieser Ansprüche in angemessenem und für den Auftraggeber erforderlichen Umfang gegen Erstattung der dem Auftragnehmer hierdurch entstehenden, nachzuweisenden Aufwände und Kosten zu unterstützen, sofern der Auftraggeber die Ansprüche nicht ohne Mitwirkung des Auftragnehmers erfüllen kann.

Der Auftragnehmer darf personenbezogene Daten ausschließlich im Rahmen der Weisung des Auftraggebers verarbeiten. Eine Weisung ist die auf einen bestimmten Umgang des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden zunächst durch die Leistungsvereinbarung und die vorliegende Vereinbarung definiert und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisung geändert, ergänzt oder ersetzt werden. Einzelweisungen, die von den Festlegungen der Leistungsvereinbarung oder der vorliegenden Vereinbarung abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers und erfolgen nach Maßgabe des in der Leistungsvereinbarung festgelegten Änderungsverfahrens, in dem auch die Übernahme etwa dadurch bedingter Mehrkosten des Auftragnehmers durch den Auftraggeber zu regeln ist.

Weisungsberechtigte Personen des Auftraggebers und der Weisungsempfänger beim Auftragnehmer werden kurzfristig jeweils mit Namen, Funktionsbezeichnung, E-Mail-Adresse und Telefonnummer der jeweils anderen Partei dieser Vereinbarung benannt.

Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen.

Der Auftragnehmer hat den Auftraggeber unverzüglich entsprechend Art. 28 Abs. 3 Unterabs. 2 DS-GVO zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind jedoch Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung und zur ordnungsgemäßen Erbringung der Leistungen gemäß dem „Wartungsvertrages“ (einschließlich der Datensicherung) erforderlich sind, sowie Kopien, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Der Auftragnehmer beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen.

Die Verarbeitung und Nutzung der Daten im Auftrag des Auftraggebers findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland statt. Eine Verlagerung in einen Staat außerhalb des Hoheitsgebiets der Bundesrepublik Deutschland bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers. Die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO bleiben unberührt.

Der Auftraggeber führt das Verarbeitungsverzeichnis gem. Art. 30 DS-GVO. Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch die in Art. 30 Abs. 2 DS-GVO genannten Informationen zur Aufnahme in das Verarbeitungsverzeichnis zur Verfügung.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

§ 5
Beachtung gesetzlicher Pflichten durch den Auftragnehmer

Neben den vertraglichen Regelungen dieser Vereinbarung und der Leistungsvereinbarung treffen den
Auftragnehmer gemäß Art. 28 DS-GVO die nachfolgenden gesetzlichen Pflichten.

- Der Auftragnehmer hat die bei der Verarbeitung von personenbezogenen Daten im Rahmen dieser Vereinbarung beschäftigten Personen gemäß Art. 28 Abs. 3 lit. b) DS-GVO schriftlich zur Vertraulichkeit zu verpflichten.
- Der Auftragnehmer hat nach Maßgabe der Art. 37 ff. DS-GVO und § 38 BDSG einen Datenschutzbeauftragten zu benennen, der seine Tätigkeit entsprechend den gesetzlichen Festlegungen ausübt. Die Kontaktdaten des Datenschutzbeauftragten sind dem Auftraggeber zum Zwecke der direkten Kontaktaufnahme mitzuteilen.
- Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde bei dem Auftragnehmer ermittelt.
- Der Auftragnehmer unterstützt den Auftraggeber bei Kontrollen durch die Aufsichtsbehörde im Rahmen des Zumutbaren und Erforderlichen, soweit diese Kontrollen die Datenverarbeitung durch den Auftragnehmer betreffen.
- Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung von dessen Verpflichtungen gemäß Artt. 32 bis 36 DS-GVO, insbesondere bei einer Datenschutz-Folgenabschätzung des Auftraggebers inklusive einer etwa notwendigen vorherigen Konsultation der zuständigen Aufsichtsbehörde. Hierzu wird der Auftragnehmer dem Auftraggeber im Rahmen des Zumutbaren proaktiv Informationen zu den technischen und organisatorischen Maßnahmen sowie den von der Auftragsverarbeitung umfassten Datenverarbeitungsvorgängen zur Verfügung stellen. Weitere Unterstützungsleistungen bedürfen der ausdrücklichen Vereinbarung der Parteien.
- Soweit den Auftraggeber aufgrund einer Verletzung des Schutzes personenbezogener Daten gesetzliche Informationspflichten wegen eines Risikos für die Rechte und Freiheiten natürlicher Personen (insbesondere nach Art. 33 DS-GVO) treffen, hat der Auftragnehmer den Auftraggeber bei der Erfüllung der Informationspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden, nachzuweisenden Aufwände und Kosten zu unterstützen.

§6
Technische und organisatorische Maßnahmen und deren Kontrolle

Die Vertragsparteien vereinbaren die in dem Anhang „Technische und organisatorische Maßnahmen“ zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaß- nahmen gemäß Art. 32 DS-GVO. Hierbei handelt es sich 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 zu berücksichtigen. Er ist Gegenstand dieser Vereinbarung. Für den Auftragnehmer bzw. Subunternehmer finden daraus die Regelungen für Schutzstufe B Anwendung.
Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dem Anhang „Technische und organisatorische Maßnahmen“ festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem

Auftraggeber mitzuteilen.

Der Auftragnehmer wird dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte geben und die entsprechende Nachweise verfügbar machen. Aufgrund der Kontrollverpflichtung des Auftraggebers gemäß Art. 28 DS-GVO vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen nach. Der Nachweis der Umsetzung solcher Maßnahmen kann dabei auch durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO sowie Vorlage eines aktuellen Testats, von Berichten unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

Der Auftraggeber kann sich jederzeit zu Prüfzwecken in den Betriebsstätten des Auftragsnehmers zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsdatenverarbeitung einschlägigen Datenschutzgesetze überzeugen.

Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände zu informieren. Der Auftraggeber darf in der Regel eine Kontrolle pro Kalenderjahr durchführen. Hiervon unbenommen ist das Recht des Auftraggebers, weitere Kontrollen im Fall von besonderen Vorkommnissen durchzuführen.

Der Auftragnehmer erhält vom Auftraggeber eine pauschale Aufwandsentschädigung für seinen im Rahmen dieser Kontrollen anfallenden Aufwand in Höhe von 300 Euro pro Kontrolle.

Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Kontrolle, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund dieses §6 der vorliegenden Vereinbarung gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber diesem die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Konkurrenten des Auftragnehmers mit der Kontrolle beauftragen.

§7
Mitteilung bei Verstößen durch den Auftragnehmer

Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er eine Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit dieser Vereinbarung feststellt.

Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

§8
Löschung und Rückgabe von Daten

Überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftraggebers.

Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Auftraggeber, jedoch spätestens mit Beendigung der Leistungsvereinbarung hat der Auftragnehmer sämtliche in seinem Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse

sowie Datenbestände (wie auch hiervon gefertigten Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung des Auftraggebers datenschutzgerecht zu vernichten (Art. 28 Abs. 3 lit. g) DS-GVO). Gleiches gilt für Test- und Ausschussmaterial. Ein Löschungsprotokoll ist dem Auftraggeber auf Anforderung vorzulegen.

Der Auftragnehmer kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben. Nach der Aufbewahrungsfrist wird auf Anforderung dem Auftraggeber ein Löschprotokoll zur Verfügung gestellt.

§9
Subunternehmer

Aufträge an Subunternehmer durch den Auftragnehmer dürfen nur mit vorheriger ausdrücklicher schriftlicher Genehmigung des Auftraggebers vergeben werden (Art. 28 Abs. 2 DS-GVO). Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen, Transportleistungen von Post- oder Kurierdiensten sowie Geldtransportdienstleistungen, Bewachungsdienste und Reinigungsdienste. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

Wenn Subunternehmer durch den Auftragnehmer eingeschaltet werden, hat der Auftragnehmer sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmer so gestalten sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Auftraggeber und dem Auftragnehmer entspricht und alle gesetzlichen und vertraglichen Pflichten beachtet werden.

Dem Auftraggeber sind in der vertraglichen Vereinbarung mit dem Subunternehmer Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist der Auftraggeber berechtigt, auf schriftliche Anforderung vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragsnehmers zu erhalten.

§10
Schlussbestimmungen

Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Vertragspartner entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

Sollten die Daten der Dateninhaberin durch Maßnahmen Dritter beim Vertragspartner, etwa durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige

Ereignisse gefährdet werden, hat der Vertragspartner die Dateninhaberin unverzüglich zu unterrichten.

Mit Abschluss dieser Auftragsverarbeitungsvereinbarung verlieren alle etwaigen zuvor zwischen den Parteien abgeschlossenen Auftragsverarbeitungsvereinbarungen mit demselben Vertragszweck ihre Gültigkeit.

Die Einrede des Zurückbehaltungsrechts i.S.d. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der ggf. zugehörigen Datenträger ausgeschlossen.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Es gilt deutsches Recht. Gerichtsstand ist Frankfurt am Main.

Anlage 1: Zweck, Art und Umfang der Auftragsverarbeitung; Art der Daten und Kategorien betroffener Personen
[Diese Angaben sind grundsätzlich vom Auftraggeber vor Abschluss des Rahmenvertrags auszufüllen]

1. Der Auftraggeber hat den Auftragnehmer mit der Erbringung von Leistungen beauftragt. Diese bestehen im Einzelnen aus den nachfolgend beschriebenen Leistungen

Dem Auftragnehmer wird ein Portal (Software as a Service Angebot) zur Verfügung gestellt über das es ihm möglich ist, Besucher und Mitarbeiter seines Unternehmens elektronisch zu erfassen und diese Daten für einen späteren Zugriff im Rahmen der Corona Pandemiebekämpfung zu speichern.

im Einzelnen spezifiziert.

2. Im Rahmen der Leistungserbringung nach dem vorgenannten Rahmenvertrag besteht für den Auftragnehmer die Möglichkeit zum Zwecke der Vertragserfüllung Einblick in und Zugriff auf folgende personenbezogene Daten zu erhalten, für die der Auftraggeber Verantwortlicher ist:

Personenstammdaten (Name, Anschrift, Geburtsdatum etc.)

Kommunikationsdaten (wie z. B. Telefon, E-Mail)

Kundenhistorie

3. Folgende Kategorien betroffener Personen sind von der Auftragsverarbeitung umfasst:

Kunden

Mitarbeiter

Anhang „Technische und organisatorische Maßnahmen“

zur Sicherstellung des Schutzes personenbezogener oder -beziehbarer Daten in der Datenverarbeitung des Auftraggebers.

1. Erforderlichkeit von Schutzmaßnahmen

1.1 Gesetzliche Grundlagen

Gemäß Art. 32 DS-GVO sind bei der Verarbeitung personenbezogener Daten die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um den Schutz des einzelnen Betroffenen vor einer Beeinträchtigung seines Persönlichkeitsrechts zu gewährleisten.

Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht (vgl. dazu oben §6). Um festzustellen, welche Maßnahme in diesem Sinne verhältnismäßig sind, wird der Benutzeraccount anhand der Daten, auf die er Zugriff hat, Schutzstufen zugeordnet, für die jeweils die grundsätzlich erforderlichen Maßnahmen festgelegt sind.

1.2 Grundlagen der Zuordnung zu den Schutzstufen

Für die Beurteilung der Schutzbedürftigkeit der personenbezogenen Daten sind die folgenden Gesichtspunkte maßgeblich:

- die Sensibilität der gespeicherten personenbezogenen oder –beziehbaren Daten
- der Umfang ihrer Auswertbarkeit
- die Möglichkeit der Verknüpfung mit anderen personenbezogenen oder personenbeziehbaren Daten.

Diese Aspekte sind bei der Bewertung generell zu berücksichtigen. Die nachfolgende Klassifizierung in Schutzstufen soll die Beurteilung im Einzelfall insoweit erleichtern, kann sie jedoch nicht ersetzen.

Hat der Benutzeraccount nur eingeschränkten Zugriff auf bestimmte Daten oder auf bestimmte Felder einer Datenbank, so erfolgt die Zuordnung zu einer Schutzstufe im Hinblick auf die Zugriffsrechte. Ergibt die Beurteilung mehrere mögliche Zuordnungen, so ist die höchstrangige maßgebend. Sollten gesetzliche Vorschriften den Schutz der Daten gesondert regeln, ist die höchstrangige Schutzmaß- nahme maßgebend.

1.3 Folgen der Einstufung

Nach der Zuordnung eines Benutzeraccounts zu einer bestimmten Schutzstufe sind die zu ergreifenden Maßnahmen dem Maßnahmenkatalog zu entnehmen.

Die aufgeführten Maßnahmen sind nicht in jedem Falle zwingend. Die Verhältnismäßigkeit ist auch gewahrt, wenn die gleiche Schutzwirkung durch gleichfalls geeignete andere Maßnahmen erreicht werden kann. In diesen Fällen legen die Datenschutzbeauftragten einvernehmlich unter Wahrung der

Beteiligungsrechte des Betriebsrats solche Sicherheitsmaßnahmen fest. Und dokumentieren diese.

2. Klassifizierung der Schutzstufen

Es wird zwischen vier Klassen von Daten unterschieden:

Schutzstufe A:

Daten, die keine oder lediglich öffentlich zugängliche personenbezogene Angaben enthalten und deren Verwendung weder durch eine freie Auswertung noch durch Verknüpfung mit anderen Dateien eine Beeinträchtigung des Persönlichkeitsrechts erwarten lässt.

Schutzstufe B:

Daten mit personenbezogenen Angaben, deren Verwendung keine besondere Beeinträchtigung des Persönlichkeitsrechts erwarten lässt, weil sie sich z.B. auf

- Name, Vorname
- Berufsbezeichnung/ Titel
- Anschrift/ Telefonnummer

- Geburtsdatum
- Zugehörigkeit zu einer bestimmten Personengruppe

(soweit diese Daten nicht im Einzelfall einer höheren Schutzstufe zuzuordnen sind) beschränken und zugleich eine Verknüpfung mit anderen personenbezogenen oder -beziehbaren Daten im organisatorischen Umfeld nicht in Betracht kommt.

Schutzstufe C:

Daten mit personenbezogenen Daten, deren Verwendung den Betroffenen

- in seiner gesellschaftlichen oder beruflichen Stellung oder
- in seinen wirtschaftlichen oder sozialen Verhältnissen beeinträchtigen kann.

Dies betrifft Daten mit Angaben über berufliche (z.B. Bezüge, Dienstreisen) und persönliche (z.B. Wohnverhältnisse, Konfession, Familienstand, Schul- und Ausbildungszeugnisse) Umstände, sofern sie nur eingeschränkt ausgewertet werden können und die Verknüpfung mit anderen personenbezogenen oder –beziehbaren Daten im organisatorischen Umfeld nicht in Betracht kommt.

Schutzstufe D:

Daten mit personenbezogenen Angaben, deren Verwendung den Betroffenen

- in seiner gesellschaftlichen oder beruflichen Stellung

oder

- in seinen wirtschaftlichen oder sozialen Verhältnissen erheblich beeinträchtigen kann.

Dazu gehören insbesondere Daten, die sich auf

- rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person (Art. 9 Abs. 1 DS-GVO)
- Straf-, Ordnungswidrigkeiten oder Disziplinarverfahren (vgl. Art. 10 DS-GVO
- dienstliche Beurteilungen, soweit sie über die Erstellung hinaus gespeichert werden, beziehen oder die einem Amts- oder Berufsgeheimnis unterliegen.
- Weiterhin alle Dateien mit Angabe, die durch Verknüpfung und freie Auswertbarkeit die Möglichkeit beinhalten, Persönlichkeits- oder Verhaltensprofile zu erstellen.

3. Erforderliche organisatorische und technische Maßnahmen

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, insbesondere hinsichtlich Vernichtung, Verlust, Veränderung oder der unbefugten Offenlegung von beziehungsweise des unbefugten Zugang zu personenbezogenen Daten, werden die nachfolgenden technischen und organisatorischen Maßnahmen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen schließen unter anderem unter Berücksichtigung der vorgenannten Kriterien Folgendes ein:

a) Maßnahmen zur Pseudonymisierung und Verschlüsselung personenbezogener Daten;
b) Maßnahmen zur dauerhaften Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung;
c) Maßnahmen zur raschen Wiederherstellung der Verfügbarkeit der personenbezogenen Daten und des Zugangs zu ihnen bei einem physischen oder technischen Zwischenfall;
d) Maßnahmen zur Sicherstellung, dass natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten;

Die nachfolgend genannten technischen und organisatorischen Maßnahmen werden regelmäßig hinsichtlich ihrer Wirksamkeit zur Gewährleistung der Sicherheit der Verarbeitung überprüft, bewertet und evaluiert (Art. 32 Abs. 1, Abs. 2, Abs. 4 DS-GVO).

3.1 Maßnahmen, die für alle Schutzstufen gelten

3.1.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle

Diese Maßnahmen sollen gewährleisten, dass Unbefugten der “körperliche” Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, verwehrt wird.

- Elektronisches Zutrittskontrollsystem
- Sicherheitstüren und/oder -fenster
- Gitter vor Fenstern und Türen
- Werkschutz, Pförtner
- Alarmanlage
- Videoüberwachung
- Spezielle Schutzvorkehrungen für den Serverraum

Zugangskontrolle

Diese Maßnahme soll das Eindringen Unbefugter in die DV-Systeme verhindern.

- Verwendung komplexer Kennwörter.
- Sperrung von IP Adressen nach einer bestimmten Anzahl falscher Anmeldungen pro Zeiteinheit.
- Verwendung personalisierter Zugänge

Zugriffskontrolle

- Sicherung aller auf Datei- und Druck-Servern gespeicherten Anwenderdaten durch Verschlüsselung,
- benutzerspezifische, abgestufte Rechteverwaltung auf Unterverzeichnis- und Dateiebene.
- Die Ausführung von nicht zugelassenen Programmdateien oder Installationsprozeduren, auch über Diskettenlaufwerk oder CD- Laufwerk wird durch technisch geeignete Maßnahmen wie Schutzsoftware verhindert,
- Bildschirmschoner auf dem Bildschirmarbeitsplatz mit Passwort- Eingabe.

Trennungskontrolle

Zweckbezogene Verarbeitung personenbezogener Daten soll technisch sichergestellt werden, d.h. zu unterschiedlichen Zwecken erhobene Daten sollen auch entsprechend getrennt verarbeitet werden.

- Getrennte Datenbanken
- Verwendung von Zugriffsberechtigungen

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 entsprechende technischen und organisatorischen Maßnahmen unterliegen.

- Pseudonymisierung der IP Adressen in den Webserver Logfiles. Täglich werden in den Webserver Logfiles die letzte Stelle der IPv4 oder IPv6 Adresse entfernt. Die IP Adresse ist dadurch nicht mehr eindeutig

3.1.2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle

- Daten werden bei der Übertragung vor unbefugter Kenntnisnahme durch Verschlüsselung oder VPN Verbindungen geschützt.
- Bei Datenträgertransporten werden die erforderlichen Sicherheitsvorkehrungen beachtet.
- Schnittstellen von PCs und externe Laufwerke (mobile Festplatten, USB-Sticks etc.) werden gegen Missbrauch geschützt.
- Eine sichere Löschung, Vernichtung und Entsorgung von Datenträgern ist gewährleistet.
- Bei Außerbetriebnahme von Geräten: Softwareseitige Löschung der Daten mit Algoritmus; physische Zerstörung der Festplatten/Speichermedien.
- Der Zugriff auf die Kundendaten und Kundensysteme bei Fernwartung erfolgt nur über sichere Leitungen (VPN).
- Bei Fernwartung ist eine sichere Identifizierung/Authentifizierung gewährleistet.
- Verwendung von Zugriffsberechtigungen

Eingabekontrolle

- Einwahlvorgänge in Kundensysteme werden protokolliert und überwacht.
- Die Eingabe von Daten im System zur Verwaltung der Kundendaten (SLX) werden protokolliert.

3.1.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

- Kundendaten sind durch geeignete Sicherungsverfahren vor Zerstörung und Verlust geschützt. Redundanz der Speichersysteme (alle Daten liegen auf zwei Speichersystemen). Zusätzlich RAID-Verfahren für Datenspeicher. Backups durch die Software veeam. Dadurch ist eine schnelle Widerherstellung von Systemen gewährleistet.
- Sicherungsbestände werden in einem getrennten Brandabschnitt verwahrt.
- Maßnahmen zur Sicherung des Serverraums und der IT-Infrastruktur: Unterbrechungsfreie Stromversorgung mit Überspannungsschutz, Klimaanlage mit Überwachung der Funktionen, Branderkennung, Brandschutz, Feuerlöscheinrichtungen, automatische Stromabschaltung
- Führen eines Notfallhandbuchs.

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

- Backups durch die Software veeam. Dadurch ist eine schnelle Widerherstellung von Systemen gewährleistet.
- Es werden zwei Rechenzentren an unterschiedlichen Standorten betrieben, so können auch in einem Desasterfall die Daten wieder zugänglich gemacht werden.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management;

  Ein betrieblicher Datenschutzbeauftragter ist bestellt und übt seine Tätigkeit weisungsfrei aus.

  Die technischen und organisatorischen Maßnahmen werden regelmäßig auf ihre Wirksamkeit hin überprüft und ggf. an technische Entwicklungen angepasst.

  Systeme werden regelmäßig entsprechend den Herstellervorgaben gepatcht und sicherheitsrelevante Updates eingespielt.

  Die Mitarbeiter werden im Zuge der Neueinstellung und während der Dauer der Beschäftigung im Turnus von einem Jahr wiederholt in den Bestimmungen des Datenschutzes unterwiesen.

- Incident-Response-Management;

  Es bestehen im Rechenzentrum Notfallpläne u.a. für folgende Szenarien:

- Brand, Wassereinbruch
- Stromausfälle
- Unerlaubte Systemzugriffe
- Einbruch, Diebstahl

- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);

  Im Rahmen der Fernwartung obliegt die Gewährung des Zugangs zu Systemen des Auftraggebers dessen Vorgaben und Einschränkungen.

Auftragskontrolle

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.