Vertrag zur Auftragsverarbeitung

gemäß Art. 28 EU-DSGVO

zwischen der

_____
Firmenname

_____
Straße, Hausnummer

_____
Postleitzahl, Ort

- Verantwortlicher - nachstehend Auftraggeber genannt -

und der

YellowMap AG
CAS-Weg 1-5, 76131 Karlsruhe
- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

1. Gegenstand und Dauer des Auftrags

Der Gegenstand des Auftrags ergibt sich aus der/s geschlossenen

- ☐ Leistungsvereinbarung
- ☐ ServiceLevelAgreement (SLA)
- ☐ Wartungsvertrags
- ☐ Partnervertrags
- ☐ Projektauftrag/-vertrag
- ☒ Produkteinsatzes SmartMaps
- ☐ _____

auf die/den hier verwiesen wird (im Folgenden Leistungsvereinbarung).
Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Konkretisierung des Auftragsinhalts

2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

2.2 Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- ☐ Adressdaten / Personenstammdaten (inkl. Position und Titel)
- ☐ Kommunikations- und Kontaktdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Auftragsdaten, Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertriebsinformationen (z.B. Leads, Projektinformationen)
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Bankdaten
- ☐ Gesundheitsdaten
- ☐ Sozialversicherungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Personen- und Kommunikationsdaten aus Filialstandorten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☒ IP-Adresse _____
- ☐ _____

- ☐ _____

Kategorien betroffener Personen
Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☐ Kunden
- ☐ Interessenten
- ☐ Abonnenten
- ☐ Mitarbeiter / Beschäftigte
- ☐ Bewerber
- ☐ Lieferanten
- ☐ Dienstleister / Vertriebs- und Integrationspartner
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ☐ Webseitenbesucher

- ☐ _____

- ☐ _____

3. Technisch-organisatorische Maßnahmen

(1) 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 zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 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 DSGVO zu berücksichtigen. Die vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sind durch diesen in schriftlicher Form zu dokumentieren. Die Dokumentation ist dieser Vereinbarung als Anlage 1 beigefügt.

(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 Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen innerhalb der gesetzlichen Frist an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft innerhalb der gesetzlichen Frist durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.
b) Die jeweils aktuellen Kontaktdaten des Datenschutzbeauftragten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.
c) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 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 auftragsrelevanten personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
d) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anlage 1].
e) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
f) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
g) 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.
h) 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.
i) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. 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 darf Unterauftragnehmer (weitere Auftragsverarbeiter) nach vorheriger schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Der Auftraggeber stimmt der Beauftragung der in Anlage 2 aufgeführten Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zu.
Die weitere Beauftragung eines neuen oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und

eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

(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.

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, in Absprache 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 nach Art. 28 DSGVO 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, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) 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
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen (Kapitel 3 DSGVO) zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen innerhalb der gesetzlichen Frist zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber kurzfristig (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 solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. 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) Nach Beendigung des Vertragsverhältnisses oder früherer Aufforderung durch den Auftraggeber wird der Auftragnehmer dem Auftraggeber auf Wunsch die mit dem Vertragsverhältnis im Zusammenhang stehenden Daten elektronisch übergeben und anschließend in seinen Datenverarbeitungsanlagen löschen. Wenn eine gesetzliche Vorschrift eine über das Vertragsende hinausgehende Aufbewahrung vorschreibt, ist der Auftraggeber für die Einhaltung der entsprechenden gesetzlichen Aufbewahrungsfristen verantwortlich.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Haftung

(1) Für Schäden des Auftraggebers durch schuldhafte Verstöße des Auftragnehmers gegen diesen Vertrag sowie gegen die ihn treffenden gesetzlichen Datenschutzbestimmungen gelten die gesetzlichen Haftungsregelungen. Soweit Dritte Ansprüche gegen den Auftraggeber wegen der nachweisbar durch den Auftragnehmer verursachten Verletzung datenschutzrechtlicher Vorschriften geltend machen, die ihre Ursache in der vertragswidrigen Erhebung oder Verwendung von Auftraggeber-Daten haben, stellt der Auftragnehmer den Auftraggeber von diesen Ansprüchen auf Anfordern frei.

(2) Der Auftragnehmer trägt die Beweislast dafür, dass etwaige Schäden nicht auf einem von ihm zu vertretenden Umstand beruhen, soweit die Schadensursache in der Erhebung oder Verwendung von Auftraggeber-Daten nach diesem Vertrag besteht.

12. Schlussbestimmungen

(1) Änderungen, Ergänzungen und die Aufhebung dieses Vertrags bedürfen der Schriftform. Gleiches gilt für eine Änderung oder Aufhebung des Schriftformerfordernisses.

(2) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und den Anforderungen des Art. 28 EU-DSGVO am besten gerecht wird.

(3) Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere der Leistungsvereinbarung, gehen die Regelungen dieses Vertrags vor.

(Ort, Datum)	Karlsruhe, den (Ort, Datum)
(Unterschrift Auftraggeber)	Christian Nickel Digital unterschrieben von Christian Nickel CN: cn=Christian Nickel, o=YellowMap AG, email=christian.nickel@yellowmap.de, c=DE Datum: 2024.09.30 09:29:32 +02'00' (Unterschrift Auftragnehmer)

Anlage 1: Technisch-organisatorische Maßnahmen

1. Vertraulichkeit

1.1. Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen:

- Wachdienst mit Verbindung zur Polizei
- Installierte und aktive Bewegungsmelder
- Gebäude-Zugang überwiegend nur mit Chip-Key
- Zentrales Schließsystem mit Sicherheitsschlössern
- Zugang in den Serverraum nur für Berechtigte
- Zentrale EDV und IT-Systeme überwiegend in Rechenzentrum ausgelagert (DIN ISO/IEC 27001:2005) (Housing):
    1. Gebäude mit Zaun, Stacheldraht, Gitter, Rolltor und Schleusensystem abgesichert
    2. Zutritt nur mit Chipkarten, PIN und Schlüssel
    3. Elektronisches Schließsystem
    4. Alarmanlagen
    5. Videoanlagen
    6. Verschlossene Server-Racks

1.2. Zugangskontrolle

Keine unbefugte Systembenutzung durch:

- Sichere, komplexe Kennwörter und Kennwortrichtlinie
- Automatische Sperrung (z.B. Kennwort oder Pausenschaltung)
- Einrichtung eines Benutzerstammsatzes pro User
- Verschlüsselung von Datenträgern
- User-ID- Abfrage mit Passwort
- Passwortkonvention: mindestens 12 Zeichen mit Sonderzeichen, Zahlen, Groß-/Kleinschreibung
- Aktivitätsprotokolle

1.3. Zugriffskontrolle

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

- Berechtigungs- und Administrationskonzept vorhanden
- Zugriffsprotokolle per Protokoll mit Logging von Richtlinienverstößen
- Passwortgeschützter Bildschirmsperre, zeitgesteuerte Aktivierung

1.4. Trennungskontrolle

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

- Getrennte Datenbanken für Unternehmen und Kunden
- Erstellung eines Berechtigungskonzepts
- Festlegung von Datenbankrechten
- Trennung Produktiv- und Testsystem

1.5. 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.

- Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder für Testzwecke möglichst zu anonymisieren / pseudonymisieren
- Sofern Loggingdaten z.B. zur Verbesserung der Services oder zu Abrechnungszwecken erhoben werden, werden diese nur anonymisiert oder pseudonymisiert gespeichert.

2. Integrität

2.1. Weitergabekontrolle

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

- E-Mail-Übertragung mit Verschlüsselung bei Bedarf umsetzbar
  (S/MIME, PDF-Verschlüsselung 256bit)
- Festplattenverschlüsselung
- Verschlüsselung der Datenwege bei Fernwartung (VPN, HTTPS)
- Anhänge in den E-Mails können bei Bedarf mit den aktuellen Verschlüsselungsprogrammen verschlüsselt werden
- Verschlüsselung von Datenträgern für einen evtl. Datenträger-Transport/-Versand

2.2. Eingabekontrolle

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

- Alle Eingaben/Änderungen im zentralen CRM CAS genesisWorld werden protokolliert
- Protokollierung von Löschungen im CRM
- Vergaben von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Umsetzung im Rechenzentrum: granulares Berechtigungskonzept für Kunden-Logins und Administrationskonzept vorhanden

3. Verfügbarkeit und Belastbarkeit

3.1. Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust:

- Zentrale EDV in Rechenzentrum ausgelagert (DIN ISO/IEC 27001:2005) (Housing)
- Datensicherungskonzept mit Vollsicherungen und Inkrementellen Sicherungen, Virtualisierung
- Ablage der Sicherungen in getrennter Brandschutzzone
- Zusatzsicherungen und getestete Rücksicherungen
- RAID-Festplattenspeicher
- Virenscanner und mehrstufige Firewalls
- Serverraum-Klimatisierung, USV, Stickstoff-Löschanlage, Brandmelder (RZ)
- Absicherung des gesamten RZs/Server mit USV sowie Notstrom-Diesel
- Spiegelung der Daten in einen 2. Brandabschnitt
- Backup-To-Disk mit Notfall-Inbetriebnahme von virtuellen Maschinen direkt aus dem Backup
- Auslagerung der Datensicherung (Ortstrennung)
- Signatur-basiertes IPS (Intrusion Prevention System) für Web-Zugriff auf CAS-eigene Dienste
- Definierte Meldewege und Notfallpläne zum Wiederanlauf
- Zentrales Monitoring von Verfügbarkeit, Auslastung, Temperatur der Systeme inkl. Eskalations-Management (E-Mail → SMS)
- Periodische Sicherheitsprüfungen bei der Entwicklung und im Betrieb des Systems z.B. mittels Penetration Tests

3.2. Rasche Wiederherstellbarkeit

- Rasche Wiederherstellung der von Daten aus mehrfach pro Tag erstellten s.g. „Snapshots“

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1. Datenschutz-Management

- Softwarelösung für Datenschutz-Management im Einsatz
- Externer Datenschutzbeauftragter

  DATENSCHUTZ perfect GmbH, Karlsruhe

  Thomas Heimhalt; Kontakt: ym-datenschutz@yellowmap.de
- Interner Arbeitskreis von Datenschutz-Verantwortlichen der verschiedenen Firmenbereiche
- Klare Verantwortlichkeiten bei Schulung/Informierung von Mitarbeitern und Erarbeitung der notwendigen Maßnahmen
- Mitarbeiter auf Vertraulichkeit / Datengeheimnis verpflichtet
- Jährliche Überprüfung der technischen Schutzmaßnahmen

4.2. Incident-Response-Management

- Einsatz von Firewall und regelmäßige Aktualisierung
- Einsatz von Spamfilter und regelmäßige Aktualisierung
- Einsatz von Virenscanner und regelmäßige Aktualisierung
- Aufgaben- und Checklisten der technischen Bewältigung von Sicherheitsverletzungen
- Hinzuziehung des externen Datenschutz-Beauftragten bei Sicherheitsverletzungen
- Einsatz von IPS (Intrusion Prevention System) und regelmäßige Aktualisierung für Haussysteme

4.3. Datenschutzfreundliche Voreinstellung

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind

4.4. Auftragskontrolle

Keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers:

- Verwendung der getroffenen Maßnahmen abhängig vom Auftrag
- Schriftlich bestellter externer Datenschutzbeauftragter mit Stellvertreter
- Einhaltung und Umsetzung der Vorgaben der EU-DSGVO
- Eindeutige Vertragsgestaltung
- Strenge Auswahl des Dienstleisters
- Vorabüberzeugungspflicht

Anlage 2: Unterauftragnehmer

Unterauftragneh-mer	**Tätigkeiten**	**Zweck**	**Kategorien von Daten**	**Betroffene**
Muttergesellschaft CAS Software AG CAS-Weg 1-5 76131 Karlsruhe	Infrastruktur für Auftragnehmer IT	Erbringung der Tätigkeiten	Siehe Kapitel 2 (2)	Siehe Kapitel 2 (2)