Technisch-organisatorische Maßnahmen

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

1. Zutrittskontrolle

Maßnahmen, die verhindern sollen, dass Unbefugte Zutritt zu Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet oder genutzt werden.
Verarbeitung eigener Daten (insb. Vertrieb, Verwaltung, Personal): Die Verarbeitung eigener Daten erfolgt in geschützten Verwaltungsräumen, die durch eine Alarmanlage geschützt sind.
Verarbeitung von Kundendaten im Rechenzentrum: Die Verarbeitung der Daten von iPrax Systems GmbH & Co. KG erfolgt in einem zertifizierten Hochsicherheitsrechenzentrum in München. Es besteht eine aktuelle Zertifizierung des Rechenzentrums nach ISO 27001 und ISO 9001. Ein rechtskonformer Vertrag im Rahmen der Auftragsdatenverarbeitung (Art. 28 DSGVO) mit erfolgter Erstkontrolle besteht.
Überwachung der Außenhaut und Firmengelände:

- Glasbruchsensoren
- 24 x 7 Sicherheitsüberwachung durch Überwachungskameras auch in Infrarot
- Vergabe von Zutrittskarten nur über spezielles Freigabeverfahren mit Ausweiskontrolle
- Vollständig elektronisches Zutrittskontrollsystem basierend auf berührungslosen Zutrittskarten mit Foto und PIN Tastencodes
- Speicherung der Zutrittsdaten über 12 Monate, Kameraaufnahmen über mehrere Monate.

Überwachung im Rechenzentrum:

- 24 x 7 Sicherheitsüberwachung durch Überwachungskameras auch in Infrarot
- Vollständig elektronisches Zutrittskontrollsystem basierend auf berührungslosen Zutrittskarten mit Foto und PIN Tastencodes
- Biometrische Handflächenscanner bei der Colocationsfläche
- Verschlossene Colocation Suites mit berührungslosen Zutrittskarten mit Foto und PIN Tastencodes
- Verschlossene Serverschränke
- Einbruchsmeldesystem an Fluchtwegen und Notausgängen
- Speicherung der Zutrittsdaten über 12 Monate, Kameraaufnahmen über mehrere Monate.

2. Zugangskontrolle

Maßnahmen, die sicherstellen sollen, dass nur befugte Personen Zugang zu Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet werden.
Verarbeitung eigener Daten: Die Verarbeitung eigener Daten findet in den Räumlichkeiten der iPrax Systems GmbH & Co KG statt, sowie für Präsentationen und Verwaltungszwecke auch auf Notebooks mit bestehender Datenverschlüsselung.
Verarbeitung von Kundendaten im Rechenzentrum:

- Transport von Daten: Der Transport von Daten findet ausschließlich per Netzwerk statt. Alle hierbei eingesetzten Verbindungen sind per SSL/IP-Sec verschlüsselt. Es werden grundsätzlich keine mobilen Geräte für den Transport von Daten von Auftraggebern eingesetzt. Für die Administration eingesetzte Computer sind mittels Datenverschlüsselung gegen unbefugte Nutzung geschützt.
- Sicherheitsprotokolle: Es werden Security Logs der Systeme aufgezeichnet und automatisiert ausgewertet und ggf. eskaliert.
- Sicherung von Bildschirmarbeitsplätzen: An allen Arbeitsplätzen des Unternehmens setzt nach 900 Sekunden ohne Eingaben automatisch ein passwortgeschützter Bildschirmschoner ein. Diese Maßnahme ist soweit möglich technisch erzwungen.
- Schutz vor externem Zugriff: Die IT-Systeme sind durch Firewall, Intrusion Prävention Systeme und Netzwerksegmentierung gegen unbefugten Zugriff geschützt. Verschlüsselter Remote-Zugriff ist nur eigenen Mitarbeitern ermöglicht.
- Vernichtung von Datenträgern: Nicht mehr benötigte Daten werden sicher gelöscht, sofern keine anderen Weisungen der Auftraggeber bestehen. Die Standardzeit für die Löschung von personenbezogenen Daten beträgt 14 Tage bei Sozialdaten und 90 Tage bei personenbezogenen Daten nach der Vertragserfüllung. Defekte Datenträger werden fachgerecht unter Beachtung der datenschutzrechtlichen Anforderungen vernichtet.

3. Zugriffskontrolle

Maßnahmen, um sicherzustellen, dass berechtigte Personen nur auf solche personenbezogene Daten Zugriff erhalten, für die sie die Befugnis zur Einsichtnahme und zur Verarbeitung besitzen.
Verarbeitung eigener Daten: Die Verarbeitung eigener Daten findet im Rahmen des bestehenden Berechtigungskonzeptes statt. Die Verteilung von Berechtigungen erfolgt nach dem Need-To-Know-Prinzip.
Verarbeitung von Kundendaten im Rechenzentrum:

- Sicherheitsstufen: Die iPrax-Plattform wird durch mehrere Sicherheitsstufen geschützt.
- Zugriffskontrolle: Im iPrax Büro sind gesicherte Zugänge gewährleistet. Der Zugang zu den iPrax Systemen durch das Unternehmen selbst erfordert einen Benutzernamen und ein Passwort (d. h. personalisierter Nutzer). Das Passwort ist vom Auftraggeber in angemessenen Abständen zu ändern. Benutzernamen können bis zu 50 Zeichen lang sein. Passwörter sind zwischen 6 bis 50 Zeichen lang. Passwörter und können nur vom Inhaber des Passworts geändert werden. Die Applikation im jeweiligen mobilen Apple Gerät in der Praxis baut auf einer SQlite-Datenbank Infrastruktur auf. Nur der authorisierte Nutzer kann Zugang zur Anwendung erhalten. Der Zugang zur iPrax-Software erfordert einen Benutzernamen und ein Passwort (d.h. personalisierter Nutzer). Benutzernamen können bis zu 10 Zeichen lang sein. Passwörter des mobilen Apple Geräts sind maximal 4 Zeichen lang. Darüber hinaus findet eine weitere Identifizierung über die Kundennummer, die Geräte-ID und den Praxisschlüssel statt. Zusätzlich wird nach dem ersten Sync mit dem Rechenzentrum eine UUID mit 16 Zeichen als zusätzliche Identifizierung gespeichert.
- Zeitliche Sitzungsbeschränkung: Sessions mit der iPrax Plattform sind zeitlich beschränkt. Offene Sessions, die länger als 30 Minuten inaktiv sind, werden beendet.
- Kommunikations-Sicherheit: Die Kommunikation mit der Datenbank im Rechenzentrum ist SSL verschlüsselt. SSL-Zertifikate sichern Verbindung zwischen Servern und Ihren Benutzern ab.
- Sicherheit auf Datenebene (Data Security Layer): Die Serverumgebung speichert Informationen in einer Datenbank und in einem Dateisystem. Der Zugang zur Datenbank im Rechenzentrum ist passwortgeschützt, unter Verwendung von einer Authentifizierung.
- Berechtigungskonzept: Im Unternehmen besteht ein definiertes Berechtigungskonzept für a) Administration, b) Softwareentwicklung, c) Usermanagement und d) Benutzer.
- Nutzerkennungen: Es existiert eine zentrale Administration für die eingesetzten Serversysteme. Die zentrale Administration nimmt keine Tätigkeiten außer der technischen Verwaltung der Sicherheits- und Serversysteme vor (seperation of duty). Die zentrale Kundenverwaltung vergibt und überwacht die individualisierten Zugänge für Kunden und sonstige Berechtigungen zum Zugriff auf eingesetzte Systeme. Der Zugriff auf die iPrax-App ist passwortgeschützt. Der Zugriff der iPrax-App auf die Datenbank im Rechenzentrum ist zum einen durch die Kunden-ID und zum anderen durch die Verschlüsselung der gesendeten Daten mit dem Praxisschlüssel gesichert. Für die Praxen und Mitarbeiter werden ebenfalls individuelle Kennungen vergeben. Initialpasswörter hat der Inhaber unmittelbar nach Empfang zu ändern. Alle Passwörter sind individuell und geheim. Die Übermittlung der Passwörter im Rahmen einer Nutzeranmeldung erfolgt getrennt auf einem anderen Medium, als die Übermittlung des Benutzer Accounts. Alle Berechtigungen orientieren sich am tatsächlichen Bedarf der Nutzergruppen und sind entsprechend so restriktiv wie möglich ausgestaltet.
- Begrenzung/Protokollierung der Fehlversuche bei der Anmeldung: Erfolgreiche und verweigerte Anmeldeversuche werden über den Server protokolliert und im Bedarfsfall eskaliert.
- Administrationszugriff: Der verschlüsselte Remote-Zugriff auf die eingesetzten Server-Systeme ist nur für folgende Personen freigeschaltet: a) Administrator, b) Entwickler
- Administratortätigkeiten: Administrative Tätigkeiten werden überwacht, als Changelog gespeichert und nachvollziehbar gemacht. Es erfolgt eine regelmäßige Prüfung dieser Logdateien.
- Protokollierung: Dateizugriffe werden überwacht und ggf. (z. B. verweigerter Zugriff) protokolliert. Auffälligkeiten, wie mehrfach fehlgeschlagene Anmeldeversuche zur Nutzung von Hard- oder Software oder andere Abweichungen werden ebenfalls protokolliert. Die Auswertung der Protokolle erfolgt soweit möglich automatisch.

4. Trennungskontrolle

Maßnahmen, die sicherstellen, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten auch nur getrennt verarbeitet werden.
Verarbeitung eigener Daten: Innerhalb des Verwaltungssystems findet keine Verarbeitung von Auftragsdaten statt.
Verarbeitung von Kundendaten im Rechenzentrum:

- Mandantentrennung: Alle personenbezogenen Daten werden innerhalb des DV-Systems, sowohl a) im Empfang der Daten, b) Verarbeitung, als auch in der c) Auslieferung auftragsbezogen getrennt gespeichert. Für jeden Kunden werden eigene Accounts angelegt, die logisch und auf Berechtigungsebene von anderen Kunden getrennt sind.
- Trennung von Entwicklungs-, Test- und Produktionsprogrammen: Entwicklungs- und Produktionsdaten werden voneinander getrennt auf den jeweils dafür eingesetzten DV-Anlagen gespeichert.

5. Pseudonymisierung

Die gem. Art. 32 Abs. 1 lit. a DSGVO und Art. 25 Abs. 1 DSGVO zu erfolgenden Maßnahmen wie Pseudonymisierung und Verschlüsselung werden gewährleistet, um für ein dem Risiko angemessenes Schutzniveau zu sorgen. Dabei erfolgt 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.

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

1. Weitergabekontrolle

Maßnahmen, die verhindern, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können. Zudem soll überprüft und festgestellt werden können, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen der Datenübertragung vorgesehen ist.
Verarbeitung eigener Daten: Die Weitergabe eigener Daten darf nur im Rahmen der Richtlinien zur Kommunikationssicherheit erfolgen. Sensible personenbezogene Kunden- oder Sozialdaten im Rahmen von iPrax dürfen nur verschlüsselt weitergegeben werden.

Verarbeitung von Kundendaten im Rechenzentrum:

- Regelung für den Eingang von personenbezogenen Daten: Auftragsbezogene personenbezogene Daten erreichen iPrax Systems GmbH & Co. KG ausschließlich per verschlüsselter Datenfernübertragung. Es werden keine physikalischen Datenträger zum Transport eingesetzt.
- Protokollierung von Dateneingängen: Dateneingänge werden über ein Monitoring erfasst und die Server-Protokolle zu Kontrollzwecken gespeichert. Die Löschung der Protokolldaten erfolgt, wenn der Auftragszweck erfüllt ist und keine steuerrechtlichen oder anderen gesetzlichen Archivierungspflichten mehr bestehen.
- Authentisierung bei Aufträgen des Auftraggebers:

Die iPrax Systems GmbH & Co KG übermittelt dem Auftraggeber das Initialpasswort zur Benutzung des Systems ausschließlich per Post. Im Bereich der iPrax-Plattform initiieren die Benutzer die Übertragung der personenbezogenen Daten selbst durch passwortgeschützte Anmeldung und anschließender Verwendung der Software. Bei Verwendung der iPrax Software werden Daten ausschließlich verschlüsselt übertragenen.

- Auftragsspezifische Sicherheitsregelungen: Soweit spezielle Sicherheitsanforderungen durch Kunden im Rahmen der Auftragsdatenverarbeitung vereinbart wurden, werden diese in den jeweiligen Abteilungen entsprechend umgesetzt und dokumentiert.
- Datenschutzgerechte Verträge mit Dritten: Soweit eine Beauftragung von Dritten erfolgt, erfolgt dies transparent gegenüber dem Auftraggeber. Es werden nur datenschutzrechtlich erforderlichen Verträge geschlossen, die mindestens den Anforderungen der Verträge zwischen Auftraggeber und Auftragnehmer dieses Vertrages entsprechen. Dokumentierte Erstprüfungen und laufende Prüfungen der Auftragnehmer erfolgen.
- Verpflichtung der Mitarbeiter auf das Datengeheimnis: Alle Mitarbeiter des Auftragnehmers sind datenschutzrechtlich zur Verschwiegenheit verpflichtet.

Es bestehen folgende Verpflichtungserklärungen im Unternehmen:

- Verpflichtungserklärung / Vertraulichkeitserklärung Datenschutz. Es wird im Sinne des Art. 28 Abs. 3 lit b) DSGVO gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben.
- Verpflichtungserklärung Vertraulichkeitserklärung Telekommunikationsgeheimnis gem. § 88 TKG (Telekommunikationsgesetz);
- Verpflichtungserklärung Vertraulichkeitserklärung Geschäftsgeheimnis (Gesetz zum Schutz von Geschäftsgeheimnissen – GeschGehG);
- Verpflichtungserklärung Sozialgeheimnis § 35 SGB I (Sozialgesetzbuch I)

2. Eingabekontrolle

Maßnahmen, um zu ermöglichen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungsanlagen eingegeben, verändert oder entfernt worden sind.
Verarbeitung eigener Daten: Die Eingabekontrolle beim Serversystem erfolgt über Changelogs. Änderungen innerhalb des Dateisystems werden sichergestellt.
Verarbeitung von Kundendaten im Rechenzentrum:

- Protokollierung von Dateneingaben: Soweit personenbezogene Daten im Auftrag des Auftraggebers empfangen und verarbeitet werden, wird dies über das bestehende Monitoring erfasst und protokolliert. Die Löschung der Protokolldaten erfolgt, wenn der Auftragszweck erfüllt ist und keine steuerrechtlichen oder anderen gesetzlichen Archivierungspflichten mehr bestehen.
- Protokollierung von Datenveränderungen: Veränderungen in den Datenbanken werden protokolliert. Die Löschung der Protokolldaten erfolgt, wenn der Auftragszweck erfüllt ist und keine steuerrechtlichen oder anderen gesetzlichen Archivierungspflichten bestehen.
- Definierte Abläufe für den IT-Betrieb: Über bestehende Prozesse, die die Tätigkeiten insb. der Entwickler vorgeben, sind die Aufgaben und Vorgehensweisen für jede Rolle im Rahmen der IT- Betreuung geregelt.

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

1. Verfügbarkeitskontrolle

Maßnahmen, mit denen personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden.
Verarbeitung eigener Daten: Die Sicherung eigener Daten erfolgt im Rahmen eines bestehenden Backup- und Archivierungskonzeptes. Verschlüsselte Datensicherungsträger werden aus den Verwaltungsräumen regelmäßig ausgelagert.
Verarbeitung von Kundendaten im Rechenzentrum: Das gesamte Rechenzentrum des eingesetzten Dienstleisters ist auf höchste Verfügbarkeit ausgelegt.

- Stromversorgung: Die externe Stromversorgung erfolgt redundant über zwei selbständige Trassen von unterschiedlichen Umspannwerken. Auch intern sind alle Löschabschnitte ebenfalls redundant versorgt und räumlich getrennt (Power Distribution Units an gegenüberliegenden Gebäudeseiten). Die Verfügbarkeit der Stromversorgung liegt bei 99.99%. Sollte dennoch eine Störung eintreten, so wird die unterbrechungsfreie Stromversorgung sofort durch USV's auf Basis von Batterien sichergestellt. Nach einer Minute Stromausfall übernehmen Dieselgeneratoren die Stromversorgung. Deren Treibstoffreserven erlauben 24 Stunden Betrieb bei Volllast. Bei Absinken des Vorrats unter 75% wird automatisch aufgefüllt. Hierfür bestehen Verträge mit ortsansässigen Lieferanten, die jederzeitige Versorgung sicherstellen.
- Klimatisierung: Die ausreichend dimensionierte Klimatisierung des Rechenzentrums (Kühlleistung aktuell 3 Megawatt) ist redundant ausgelegt. Derzeit existieren 12 Central Cooling Units, von denen mindestens zwei den Rechenzentrumsbereich des RZ-Dienstleisters versorgen.
- Wartung und Überwachung der IT-Infrastruktur: Monitoringsysteme melden permanent den Zustand der IT-Infrastruktur. Bei ungewöhnlichem Verhalten wird die Problemanalyse und -Lösung, auch teils unter Hinzunahme von externen Spezialdienstleistern, vorgenommen. Hinsichtlich der RZ-Infrastruktur werden

nach den Wartungsrichtlinien quartalsweise, halbjährliche und jährliche Funktionstest einzelner Systeme durchgeführt. Bei den Dieselgeneratoren erfolgt z. B. ein monatlicher Testlauf gegen eine Lastbank, der die Funktion der Notstromaggregate bei Volllast prüft. Tests und Testergebnisse werden fortlaufend dokumentiert. Es finden automatisierte, permanente elektronische Tests der Core IT-Systeme statt, die die Funktion und Leistungsfähigkeit (z. B. den Durchsatz) prüfen. Jährlich viermal werden proaktiv Soft- und Hardwareupdates der zentralen Systeme evaluiert. Bugfixreports der Lieferanten garantieren darüber hinaus eine Prävention von Hard- und Softwarefehlern. Die Stabilität einer Hard-/Software hat Vorrang vor Featurevielfalt, wenn die Entscheidung für ein Update getroffen werden soll.

- Umwelteinflüsse, Notfallprävention, insb. Brandschutz: Das gesamte Rechenzentrum wird über ein zentrales Gebäudemanagementsystem überwacht. Es existieren automatische Meldeeinrichtungen für Wassereinbruch, Temperaturanstieg, Brandfrüherkennung und sonstige betriebsrelevanten Störungen. Auch Bereiche mit Unterbodenleitungen werden automatisch überwacht. Die Meldeeinrichtungen werden regelmäßig gewartet und auf Funktion getestet. Die Feuerlösch- und Rauchabzugsanlage wird automatisch beim Eintreten von kritischen Situationen durch mehrfach vorhandene Brandmeldeanlagen ausgelöst. Die zusätzliche optische Überwachung und die damit gegebene Möglichkeit des manuellen Eingreifens schützt die im Rechenzentrum befindlichen Systeme bestmöglich vor Beschädigungen im Brandfall. Im Gebäude werden soweit wie möglich nicht entflammbare und raucharme Materialien verwendet. Das Gebäude ist in mehrere selbständige Brandabschnitte unterteilt. Innerhalb des eigentlichen Rechenzentrumsbereichs erfolgt keine Lagerung, insbesondere von entflammbaren Materialien. Brandschutzwartungen erfolgen nach geltender Brandschutzverordnung. Betriebsrelevante Systeme wie z. B. Gebäudetechnik, USV / UPS inkl. Batterie und Generatortechnik, Klimatechnik werden nach Richtlinien der Hersteller gewartet. Notfallübungen werden im Zuge der Wartungen durchgeführt. Zusätzlich wird ein jährlicher „Black Building"-Test zur Simulation eines totalen Stromausfalls durchgeführt. Tatsächliche Störungsmeldungen werden zentral außerhalb des Rechenzentrums gesammelt und rund um die Uhr ausgewertet. Je nach Art der Störung erfolgt eine sofortige Benachrichtigung der Mitarbeiter vor Ort per E-Mail (Ticketsystem) oder telefonisch.
- Netzwerkanbindung: Glasfaser- und Kupferleitungen sind jeweils in höchstwertigen eigenen Leitungsschächten verlegt. Die Anbindung des Rechenzentrums an das Internet erfolgt mehrfach redundant über verschiedene 1 und 10 Gbit/s Ethernet Carrieruplinks sowie Peerings mit anderen Internet Service Providern und Rechenzentren. Momentan bestehen 7 Anbindungen. Die Verfügbarkeit der Anbindung liegt bei 99,95%. Backbonestörungen sind innerhalb von maximal 4 Stunden zu beheben. Internetverbindungen bestehen standardmäßig mit 1 Gbit/s, optional sind auch 10 Gbit/s möglich. Diese Bandbreiten sind garantiert bis zu den Backbones anderer Betreiber.
- Bedienter Betrieb: Der bediente Betrieb 7x24 wird gewährleistet. Sowohl für die RZ Grundleistungen wie auch für die Netzwerksysteme steht ein 7x24 Stundensupport zur Verfügung, der die Verfügbarkeit und Leistung der Systeme überwacht. Eine 24 Stundenhotline für den Kunden ist vorhanden.
- Gebäudewartung: Geplante Wartungen und andere notwendige Maßnahmen – z. B. Veränderungen an der RZ Infrastruktur – werden hinsichtlich der Beeinträchtigung verschiedenen Klassifizierungsstufen (PSA no, low und high) zugeordnet. Der Auftragnehmer wird über eine geplante und voraussichtlich Servicebeeinträchtigende Maßnahme vier Wochen im Voraus durch den RZ-Betreiber informiert.
- Datensicherung: Die Sicherung der Systeme beim beauftragten Dienstleister erfolgt in mindestens 14 Generationen. Eine Rücksicherung der Daten im Rahmen des erfolgten Backups zurückgehend durch den Dienstleister wird garantiert. Die garantierte Verfügbarkeit der Systeme beträgt im Jahresmittel mindestens 99%.
- Notfallkonzept: Der Dienstleister hat ein bestehendes Notfallkonzept in dessen Rahmen regelmäßige Test der Infrastruktur (Internetanbindung, Storage, Serverinfrastruktur) dokumentiert durchgeführt werden.
- Updates: Der Administrator versorgt alle Server und Software regelmäßig mit aktuellen Sicherheits- und sonstigen notwendigen Updates. Der Einsatz von Sicherheitsupdates erfolgt nach Tests auf separaten Testsystemen.
- Virenschutz: Im Rahmen der Gateway Security werden übertragene Daten auf den eingesetzten Servern auf Schadsoftware überwacht. Die Software hält sich selbst automatisch auf aktuellem Stand (Programm und Signaturen). Verdächtige Dateien werden automatisch in ein Quarantäne-Verzeichnis verschoben Eine rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO) wird durch die Rücksicherung der Daten im Rahmen von Backups gewährleistet.

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

1. Incident-Response-Management

Bei Sicherheitsvorfällen kann auf einen bestehenden Vorfallreaktionsplan zurückgegriffen werden. Alle verantwortlichen Personen werden auf mögliche Vorfälle vorbereitet. Dies umfasst die Identifikation des Vorfalls, die Eindämmung des Schadens, die Entfernung der betroffenen Systeme und die Wiederherstellung des Status Quo. Gewonnene Erkenntnisse werden dokumentiert und analysiert, so dass künftige Reaktionen verbessert werden können.

2. Datenschutzfreundliche Voreinstellungen

Datenschutzfreundliche Voreinstellungen gem. Art. 25 Abs. 2 DS-GVO werden proaktiv und frühzeitig implementiert, um das Schutzniveau für personenbezogene Daten in der DS-GVO zu gewährleisten. Dabei werden vor allem Zweck, Umfang, Speicherfrist und Zugänglichkeit von personenbezogenen Daten berücksichtigt. Die getroffenen Maßnahmen stellen insbesondere sicher, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

3. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur gemäß den Weisungen des Auftraggebers verarbeitet werden können.
Verarbeitung eigener Daten: Die Verarbeitung eigener Daten findet in den Büroräumen statt.
Verarbeitung von Kundendaten im Rechenzentrum: Die Verarbeitung personenbezogener Daten im Auftrag erfolgt ausschließlich im Rahmen der zugrundeliegenden Vereinbarung, entsprechend der gesetzlichen Vorschriften und nach Weisung des Auftraggebers. Soweit eine Beauftragung von Dritten erfolgt, erfolgt dies transparent gegenüber dem Auftraggeber. Es werden nur datenschutzrechtlich erforderliche Verträge geschlossen, die mindestens den Anforderungen der Verträge zwischen Auftraggeber und Auftragnehmer dieses Vertrages entsprechen. Dokumentierte Erstprüfungen und laufende Prüfungen der Auftragnehmer erfolgen.

—
Stand Mai 2023