Vertrag zur Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 DSGVO

1 Präambel

(1) Dieser Vertrag zur Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO) wird abgeschlossen zwischen der UPDATU GmbH, Fuchsbühlweg 25, 88097 Eriskirch (nachfolgend „UPDATU“ „Anbieter“ oder „Auftragnehmer“) und Ihnen (nachfolgend „Auftraggeber“ oder „Kunde“ genannt)

(2) Falls Sie diesen Vertrag im Namen einer Organisation abschließen, willigen Sie in diesen Vertrag für diese Organisation ein und sichern UPDATU zu, dass Sie die Befugnis besitzen, eine solche Organisation an diesen Vertrag und an die mitgeltenden Verträge zu binden.

2 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

(1) UPDATU verarbeitet personenbezogene Daten im Auftrag des Kunden (Auftragsverarbeitung). Dies umfasst alle Tätigkeiten, die UPDATU gemäß den Leistungsbeschreibungen und den jeweiligen vertraglichen Vereinbarungen erbringt und die eine Auftragsverarbeitung darstellen.

(2) Hierbei sind die folgenden Daten Bestandteil der Auftragsverarbeitung:

Art der Daten	**Art und Zweck der Datenverarbeitung**	**Kategorien betroffener Personen**
- Identifikationsdaten - Personenstammdaten - Kontaktdaten - Nutzer- und Rechtedaten - Datenschutz-Vorgangsdaten - Nutzungsdaten	- Management datenschutzrechtlicher Anforderungen - Optimierung der Datenqualität - Kennzahlenermittlung zur Nutzung des Dienstes	- Nutzer, welche in der UPDATU Nutzerverwaltung administriert werden - Kontakte, welche in der UPDATU Kontaktverwaltung administriert werden - Besucher, welche das UPDATU-Portal des Auftraggebers besuchen

(3) Die Verarbeitung erfolgt zeitlich unbefristet, sofern dies in den Leistungsbeschreibungen und den jeweiligen vertraglichen Vereinbarungen nicht anders vereinbart ist. Die in den jeweiligen vertraglichen Vereinbarungen geregelten Kündigungsfristen bleiben unberührt.

3 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO).

(2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird wirtschaftlich vertretbare technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DSGVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.
Für die Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüfte Wirksamkeit wird auf die vorliegende Zertifizierung nach DIN ISO 27001, sowie auf die technisch-organisatorischen Maßnahmen nach Art. 32 DSGVO in der jeweils aktuellen Version verwiesen.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Artt. 33 bis 36 DSGVO genannten Pflichten.

(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder

einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.

(6) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

(7) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

(8) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

5 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt §3 Abs. 81 entsprechend.

(3) Der Auftraggeber verpflichtet sich zur Einhaltung der Rechte der betroffenen Personen nach Artt. 12 bis 23 DSGVO Personen. Die Verpflichtung bezieht sich hierbei auf den in Ziffer 2.2 aufgeführten Kreis der betroffenen Personen.

6 Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person des Auftraggebers nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

7 Nachweismöglichkeiten

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach in Form von:
- Zertifikat zur Informationssicherheit nach DIN ISO/IEC 27001
- Dokumentation der technisch-organisatorischen Maßnahmen nach Art. 32 DSGVO

(2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen oder keine geeignete Qualifikation im Umfeld Informationssicherheit nachweisen können, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

Der Auftraggeber stimmt der Benennung eines unabhängigen externen Prüfers durch den Auftragnehmer zu, sofern der Auftragnehmer eine Kopie des Auditberichts zur Verfügung stellt. Der Auditbericht ist nach Zweckerfüllung zu löschen.

Der Aufwand einer Inspektion ist kostenpflichtig zu beauftragen und für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

(3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

8 Subunternehmen (weitere Auftragsverarbeiter)

(1) Der Einsatz von Subunternehmen im Sinne des Art. 28 Abs. 2 und 4 DSGVO als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber nicht widersprochen hat.

(2) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

(3) Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragnehmer den Auftraggeber. Der Auftraggeber kann der Änderung innerhalb einer angemessenen Frist widersprechen. Erfolgt ein Widerspruch behält sich der Anbieter das Recht der fristlosen Vertragskündigung aus wichtigem Grund vor. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben.

(4) In Notfallsituationen kann der Auftragnehmer ohne vorherige Information ein Subunterunternehmen hinzuziehen oder ersetzen, wenn dies aus Gründen der Netzwerk- oder Informationssicherheit ist. Der Auftragnehmer informiert den Auftraggeber in diesem Fall unverzüglich nach Beendigung der Notfallsituation.

9 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, 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.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Es gilt deutsches Recht.

10 Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

11 Vergütung

(1) Die Durchführung eines Audits und die Durchführung von Anweisungen des Auftraggebers, welche Kosten beim Auftragnehmer verursachen, sind vor Durchführung der Anweisung kostenpflichtig zu beauftragen.

(2) Sollte im Rahmen eines Audits ein wesentlicher Verstoß gegen diesen Vertrag zur Auftragsverarbeitung identifiziert werden, trägt der Auftragnehmer die Kosten, welche auf Seiten des Auftragnehmers entstehen.

Technisch-Organisatorische Maßnahmen

1 Übersicht

Nachhaltige Informationssicherheit ist integrativer Bestandteil des Managementsystems von UPDATU. Hierbei schützt UPDATU Ihre Daten mit technisch-organisatorischen Maßnahmen, welche laufend überprüft werden. In diesem Zusammenhang möchten wir insbesondere hervorheben:

Informationssicherheit nach ISO/IEC 27001
UPDATU wurde erfolgreich durch den TÜV Rheinland nach ISO/IEC 27001 (Informationssicherheit) zertifiziert.

Datensicherheit nach Art. 32 Abs. 1 DSGVO
Zur Erfüllung der Anforderungen nach Art. 32 Abs. 1 DSGVO beschriebt UPDATU in diesem Dokument technische und organisatorischen Maßnahmen, die erforderlich sind, um den Schutz personenbezogener Daten zu gewährleisten.

Datenschutzmanagement-System (DSMS)
UPDATU wird von der Deutschen Datenschutzkanzlei (DDSK) betreut. UPDATU nutzt das Datenschutzmanagement-System (DSMS) der Deutschen Datenschutzkanzlei, in welchem alle Maßnahmen, Verfahren und Tätigkeiten im Bereich Datenschutz abgebildet werden. Das DSMS beinhaltet datenschutzrechtlichen Vorgaben, eine umfassende Struktur zur Abbildung der Datenschutzmaßnahmen und beinhaltet darüber hinaus einen Maßnahmenplan zur rechtskonformen Umsetzung der EU-Datenschutzgrundverordnung (Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO).

Das DSMS unterliegt der ständigen Überwachung und Verbesserung (PDCA-Zyklus) nach dem Vorbild der ISO/IEC 27001.

2 Organisatorisches

UPDATU betreibt ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Datenschutzbeauftragter und Informationssicherheitsbeauftragter
Die Wirksamkeit der Maßnahmen wird u.a. durch den Datenschutzbeauftragten und durch den Informationssicherheitsbeauftragten von UPDATU laufend geprüft.

UPDATU Mitarbeiter
Alle bei der Datenverarbeitung eingesetzten Mitarbeiter sind auf das Datengeheimnis bzw. auf die Vertraulichkeit gemäß Artt. 28 Abs. 3 lit. b, 29, 32 Abs. 4 DSGVO verpflichtet

UPDATU Unterauftragnehmer
Alle bei der Datenverarbeitung eingesetzten UPDATU Unterauftragnehmer werden im Sinne des Art. 28 DSGVO beauftragt und sind ISO/IEC 27001 zertifiziert oder haben vergleichbare Zertifizierungen

Zertifikat

Prüfungsnorm **ISO/IEC 27001:2013**

Zertifikat-Registrier-Nr. **01 153 1800128**

Unternehmen:

UPDATU GmbH
Fuchsbühlweg 25
88097 Eriskirch
Deutschland

Geltungsbereich:

Entwicklung, Betrieb und Vertrieb von digitalen Lösungen und Services, sowie Support- und Beratungsleistungen.

Statement of Applicability (SoA) : 06.03.2018

Durch ein Audit wurde der Nachweis erbracht, dass die Forderungen der ISO/IEC 27001:2013 erfüllt sind.

Gültigkeit:

Dieses Zertifikat ist gültig vom 30.05.2018 bis 29.05.2021.

30.05.2018

TÜV Rheinland Cert GmbH
Am Grauen Stein · 51105 Köln

www.tuv.com

DAkkS Deutsche Akkreditierungsstelle D-ZM-16031-01-00

TÜVRheinland®
Genau. Richtig.

3 Sicherungsmaßnahmen

3.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1.1 Zutrittskontrolle

Die Zutrittskontrolle umfasst Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Ein Schutzzonenkonzept ist implementiert.
- Es ist eine verantwortliche Person für die Verwaltung der Zutrittsmittel bestimmt.
- Es bestehen Regelungen bzgl. Vergabe und Entzug von Gebäudezutrittsberechtigungen für Mitarbeiter und Besucher.
- Restriktive Zutrittsberechtigungen kommen zum Einsatz.
- Das Firmengebäude ist mit einem Schließsystem ausgestattet.
- Die Schlüssel stehen nur den Berechtigten zur Verfügung.
- Besucher halten sich in kritischen Bereichen ausschließlich in Begleitung eines Mitarbeiters im Gebäude auf

3.1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Es ist eine Benutzerverwaltung implementiert.
- Benutzerkonten werden Benutzern eindeutig zugeordnet.
- Zeitlich automatisierte Bildschirmsperren sind aktiviert.
- Es ist eine Passwortrichtlinie im Einsatz
- Die Generierung und Verwaltung von Passwörtern erfolgt über ein Passwort-Tool.
- In allen Systemen ist Zwei-Faktor-Authentifizierung aktiviert, soweit technisch möglich.
- Für Remote-Arbeitsplätze-Rechner existieren verschlüsselte Zugangsverfahren (z.B. VPN)
- Maßnahmen zur Abwehr von Angriffen sind implementiert (z.B. Firewall, Virenscanner)

3.1.3 Zugriffskontrolle

Maßnahmen die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Ein verbindliches Verfahren zur Vergabe von Berechtigungen ist implementiert.
- Es werden nur jene Berechtigungen vergeben, welche für die Aufgabenerfüllung erforderlich sind.
- Die Berechtigungsvergabe wird dokumentiert.
- Die Rechte werden durch Administratoren verwaltet.
- Berechtigungen werden bei Aufgabenwechsel innerhalb des Unternehmens überprüft und ggf. angepasst.
- Berechtigungen werden bei Austritt aus dem Unternehmen entzogen.
- Die eingesetzten Systeme haben ein dediziertes Rechtesystem, welche den unbefugten Zugriff und das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Daten verhindern.

3.1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Es ist eine Netzsegmentierung implementiert, welche Entwicklungs- und Produktionsumgebung trennt
- Der Zugriff auf die jeweilige Umgebung ist nur mit Berechtigung für jeweilige Umgebung möglich.
- Der Übergang von Entwicklungssystem zum Produktionssystem ist durch ein workflowgestütztes Genehmigungsverfahren gesichert und nachvollziehbar dokumentiert.
- Test-, Produktiv- und Backup-Daten werden getrennt verwaltet.
- Der Zugriff auf schutzwürdige Daten ist nur mit Berechtigung für jeweilige Daten möglich.
- Schutzwürdige Daten werden den Mitarbeitern nur in dem Umfang zur Verfügung gestellt, wie es für die zugewiesene Aufgabenerfüllung unbedingt erforderlich ist.

3.1.5 Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

Maßnahmen um Sorge zu tragen, dass eine Rückbeziehbarkeit von Daten auf (natürliche) Personen zumindest eingeschränkt ist.

- Die IT-Architektur und die Datenflüsse zwischen den Komponenten der IT-Architektur sind dokumentiert und Grundlage für die interne Übersicht genutzter Verschlüsselungsverfahren
- Es ist dokumentiert mit welchen Verfahren die Daten innerhalb der Komponenten verschlüsselt werden und mit welchen Verfahren der Datenaustausch zwischen den Komponenten verschlüsselt wird.
- Die Festplatten der Endgeräte werden verschlüsselt.
- Die Nutzung der Webseiten durch Webseiten-Besucher erfolgt mit Hilfe eines Verschlüsselungsverfahrens

3.2 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

3.2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Mit externen Partner erfolgt der Datenaustausch unter Nutzung von Verschlüsselungstechnologien (z.B. VPN).
- Externe Verbindungen sind nur über freigegebene Anwendungen möglich.
- Es bestehen verbindliche Sicherheitsregelungen für den Transport von vertraulichen Datenträgern (z.B. Verschlüsselung der Datenträger).
- Es werden Akten-/Datenträgervernichter bzw. Dienstleister unter Beachtung DIN 66399 oder vergleichbarer Normen eingesetzt.
- Es ist ein abschließbares Archiv zur Aufbahrung schutzwürdiger Aktien und Datenträger vorhanden.
- Es ist ein Löschkonzept für personenbezogene Daten implementiert.

3.2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Die Eingabe, Änderung und Löschung von personenbezogenen Daten wird, soweit technisch möglich und datenschutzrechtlich zugelassen, protokolliert.
- Die Protokollierung ermöglicht die Nachvollziehbarkeit, ob und durch welchen Benutzer personenbezogene Daten eingegeben, verändert gelöscht worden sind.

3.2.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

- Mit Hilfe von Monitoring-Funktionen wird eine fortlaufende Überwachung zur Auslastung der Dienste durchgeführt
- Es sind Grenzwerte für die performante Betriebsfähigkeit definiert, welche im Falle von Unter-/Überschreitung der Grenzwerte automatisiert eine Warnmeldung auslösen
- Die Server können im Falle einer erhöhter Auslastung kurzfristig auf erhöhte, kapazitative Anforderungen angepasst werden.
- Es ist ein Reifegrad-Modell implementiert, welches das Einspielen neuer Softwarestände in die Produktivumgebung erst nach Erreichen des definierten Reifegrades erlaubt
- Zur aktiven Erkennung von Incidentrisiken werden externe Warn- und Informationsdienste genutzt (z.B. CERT-Bund)
- Zur Vermeidung von Datenverlusten ist ein Datensicherungskonzept implementiert, welches automatisiert und periodisch Sicherungskopien der Produktivdaten erstellt. Die Sicherungskopien sind unveränderbar und werden auf Basis der definierten Löschfristen des Löschkonzepts vollautomatisiert gelöscht, vorbehaltlich gesetzlicher Verpflichtungen oder des Einsatzes für Zwecke der Netzwerk- und Informationssicherheit

3.2.4 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können, sowie Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden

- Es ist ein Notfallkonzept zur Notfallprävention und -bewältigung verfügbar.
- Es ist ein Verfahren implementiert, welches Betriebsstörungen automatisiert feststellt und in einer Vielzahl von Fällen auch die Betriebsfähigkeit automatisiert wiederherstellt
- Im Falle von Betriebsstörungen unbekannter Ursache, deren Gefährdungspotential nicht eingeschätzt werden kann, werden die betroffenen Module oder der gesamte Dienst so lange außer Betrieb gesetzt, bis durch geeignete Maßnahmen die Sicherheit wiederhergestellt worden ist.
- Es ist ein Recovery-Verfahren implementiert, über welches Sicherungskopien der Produktivdaten und/oder alte Softwarestände in die Produktumgebung eingespielt werden können.

3.3 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (Art. 25 Abs. 1 DSGVO; Art. 32 Abs. 1 lit. d DSGVO)

Maßnahmen, die die Qualität der technischen und organisatorischen Maßnahmen ausreichend testen, sowie Maßnahmen, die prüfen, ob erstellte Backups zur Wiederherstellung verlorener Daten genutzt werden können.

3.3.1 Datenschutz-Management

- UPDATU nutzt das Datenschutz-Managementsystem (DSMS) der Deutschen Datenschutz Kanzlei (DDSK), in dem alle Maßnahmen, Verfahren, Tätigkeiten etc. im Bereich Datenschutz abgebildet werden.
- Das DSMS beinhaltet die wichtigsten datenschutzrechtlichen Vorgaben und eine umfassende Struktur zur Abbildung der Datenschutzmaßnahmen und beinhaltet darüber hinaus einen Maßnahmenplan zur rechtskonformen Umsetzung der EU-Datenschutzgrundverordnung (Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO).
- Mitarbeiter, die als Administratoren Zugriff auf die Systeme haben, sind alle hinsichtlich des Datenschutzes belehrt, auf das Datengeheimnis verpflichtet und haben als Bestandteil ihres Arbeitsvertrags entsprechende Verschwiegenheits- und Geheimhaltungsvereinbarungen akzeptiert.
- UPDATU ist eine Lösung für das Datenschutz-Management mit Fokus auf die Erfüllung der Informationspflichten nach Art. 13 und 14 DSGVO. UPDATU nutzt die Lösung auch für unternehmenseigene Zwecke

3.3.2 Informationssicherheits-Management

- UPDATU nutzt das Informationssicherheits-Managementsystem (ISMS) der Deutschen Datenschutzkanzlei, welches die Anforderungen der ISO/IEC 27001 behandelt.
- Es ist ein ISMS eingerichtet und umgesetzt. Die Aufrechterhaltung der Informationssicherheit und deren fortlaufenden Verbesserungen werden dokumentiert.
- Informationssicherheitsrisiken werden aktiv identifiziert, beurteilt und behandelt.
- UPDATU ist nach ISO/IEC 27001 (Informationssicherheit) zertifiziert.

3.3.3 Incident-Response-Management

- Es ist ein Incident-Prozess (Behandlung von Sicherheitsvorfällen) nach Vorgabe der ISO/IEC 27001, Artt. 33/34 DSGVOimplementiert, welches u.a. Meldewege und Behandlung von Incidents regelt.
- Es wird eine workflowgestützte Lösung zur Registrierung, Dokumentation und Verfolgung von Incidents eingesetzt
- Es sind Verantwortlichkeiten für die Behandlung von Sicherheitsvorfällen definiert

3.3.4 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

- Im Kontaktmanagement des Dienstes werden nur jene personenbezogenen Daten als Pflichtfelder definiert, welche zwingend für die Erfüllung der Informationspflichten nach Artt. 13 und 14 DSGVO, sowie für die Erfüllung der Rechenschaftspflicht nach Art. 5 Abs. 2 erforderlich sind.
- Zur Vermeidung von „Privacy Fatigue“ stellt der Dienst sicher, dass im Rahmen der Durchführung der Informationspflichten durch den Auftraggeber jede betroffene Personen nicht mehrmals die gleiche Datenschutzerklärung durch verschiedene Personen aus der Organisation des Auftraggebers erhält.
- Der Dienst bietet betroffenen Personen die schnelle und einfache Möglichkeit zur Beantragung eines Löschantrags durch die betroffene Person. Dies verkürzt die Dauer ungewünschter Verarbeitung personenbezogener Daten der betroffenen Person beim Auftraggeber.

- Der Dienst ist in der Lage im Rahmen der Durchführung der Informationspflichten per Email nicht mehr aktuelle Emails von betroffenen Personen automatisch zu erkennen. Diesen Indikator kann der Auftraggeber zur proaktiven Umsetzung von datenschutzfreundliche Maßnahmen nutzen, wie z.B. die sofortige Löschung oder Aktualisierung der personenbezogenen (Stamm-)Daten.

3.3.5 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Die Beauftragung von Unterauftragnehmern im Sinne des Art. 28 DSGVO erfolgt nach strengen Kriterien, wie z.B. unter Berücksichtigung der Anforderungen der DSGVO für den internationalen Datentransfer.
- Die Beauftragung von Unterauftragnehmern unterliegt einem internen Freigabeprozess und wird dokumentiert.
- Die Prüfung der Erfüllung der technischen-organisatorischen Maßnahmen des Unterauftragnehmers im Sinne des Art. 32 Abs. 1 DSGVO erfolgt primär durch den Nachweis einer gültigen und anerkannten Informationssicherheitszertifizierung, wie z.B. ISO/IEC 27001.
- Die Gültigkeit der Zertifikate von Unterauftragnehmern wird dokumentiert und kontrolliert.
- Auf die betreffenden technischen Umgebungen werden nur restriktive Zugriffsberechtigungen vergeben. Bei externem Zugriff auf das System wird der Zugang nach Beendigung der Zusammenarbeit deaktiviert oder gesperrt.

3.3.6 Dokumentationskontrolle

Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können

- Als integrativer Bestandteil des Datenschutz-Managementsystems sind relevante Datenschutz-Dokumentationen und -Richtlinien selbstverständlich, wie z.B. das Verarbeitungsverzeichnis nach Art. 30 DSGVO
- Die gesamte Dokumentation unterliegt einem Review-Zyklus.