Allgemeine Geschäftsbedingungen (AGB)

Die Registrierung für das Online-Angebot unter <https://datenschutz-grundversorgung.de> (nachstehend auch Online-Plattform genannt) setzt voraus, dass Sie den nachfolgenden Allgemeinen Geschäftsbedingungen zustimmen. Bitte lesen Sie diese daher sorgfältig durch.

1. Geltungsbereich, Begriffsbestimmungen

(1) Diese AGB gelten für alle Vertragsbeziehung zwischen uns, der DSGrundversorgung GmbH, Ericusspitze 4, 20457 Hamburg, und Ihnen als Kunde. Die AGB sind Bestandteil aller Verträge, die wir mit unseren Vertragspartnern über die von uns angebotenen Leistungen schließen. Sie gelten auch für alle nachträglich über die Online-Plattform, telefonisch, schriftlich oder per E-Mail geschlossenen Verträge, selbst wenn sie nicht nochmals gesondert vereinbart werden.

(2) Die AGB gelten unabhängig davon, ob Sie Verbraucher (§ 13 BGB) oder Unternehmer (§ 14 BGB) sind. Der Kunde ist Verbraucher, soweit der Zweck des Abrufs unseres Online-Angebots nicht überwiegend seiner gewerblichen oder selbständigen beruflichen Tätigkeit zugerechnet werden kann. Dagegen ist Unternehmer jede natürliche oder juristische Person oder rechtsfähige Personengesellschaft, die beim Abschluss des Vertrags über unser Online-Angebot in Ausübung ihrer gewerblichen oder selbständigen beruflichen Tätigkeit handelt.

(3) Abweichende Bedingungen des Kunden akzeptieren wir nicht. Dies gilt auch, wenn wir der Einbeziehung nicht ausdrücklich widersprechen.

2. Vertragsgegenstand

(1) Bei dem unter <https://datenschutz-grundversorgung.de> abrufbaren Online-Angebot handelt es sich um eine Online-Plattform zur Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO), zur Führung der Datenschutzdokumentation sowie um eine Bibliothek von Mustern und Vorlagen aus dem Bereich Datenschutz. Optional kann ein externer Datenschutzbeauftragter bestellt werden, der die gesetzlichen Aufgaben des Art. 39 DSGVO übernimmt und die Kunden individuell berät, um die datenschutzrechtlichen Bestimmungen einzuhalten. Unsere Kunden können darüber hinaus verbleibende Risiken optional mit einer Cyber-Versicherung über die Funk Gruppe absichern.

(2) Unsere Kunden können zwischen einem kostenfreien Angebot mit reduzierten Inhalten („BASIS“, endet automatisch nach 90 Tagen), einem kostenpflichtigen Angebot mit einem Vollzugriff auf die Online-Plattform nebst Möglichkeit zum Datenexport („PLATTFORM“, monatlich kündbar) und der Beauftragung eines externen Datenschutzbeauftragten („FULL-SERVICE“, Mindestvertragslaufzeit zwei Jahre) wählen. Der Leistungsumfang richtet sich nach den vom Kunden ausgewählten Paketen/Optionen. Der Vertragsschluss für das Paket „FULL-SERVICE“ erfolgt individuell nach Kontaktaufnahme und ist nicht direkt über die Online-Plattform möglich.

(3) Nach Maßgabe dieser AGB sind wir verpflichtet, die vom Kunden ausgewählten Leistungen während der Vertragslaufzeit zu erbringen.

3. Registrierung, Vertragsschluss

(1) Die Präsentation und Bewerbung der Leistungen auf unserer Website stellen kein verbindliches Angebot zum Vertragsschluss dar.

(2) Voraussetzung für die Nutzung unseres Online-Angebots ist die Bestätigung der Registrierung des Kunden durch uns. Der Kunde kann zwischen folgenden Leistungen wählen:

a) Mit der Registrierung erhält der Kunde kostenfreien Zugriff auf die Online-Plattform für 90 Tage mit folgenden Leistungen („BASIS“):

- Test der Online-Plattform (kostenlos, teilweise eingeschränkte Funktionen)
- Software zur Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten
- Muster & Vorlagen (Auswahl)
- Dateiverwaltung zur Datenschutzdokumentation
- Kein Risiko, der Test endet automatisch nach 90 Tagen

Der Kunde gibt seine verbindliche Vertragserklärung durch Anklicken des Buttons "REGISTRIEREN >>" ab. Der Vertrag kommt durch Bestätigung der Registrierung des Kunden durch uns zustande. Wir können die Bestätigung der Registrierung auch durch Freischaltung der Zugangsdaten des Kunden erklären.

b) Registrierte Kunden haben die Möglichkeit, einen Vollzugriff auf die Online-Plattform nebst Möglichkeit zum Datenexport mit folgenden Leistungen zu erwerben („PLATTFORM“):

- Nutzung der Online-Plattform
- Software zur Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten
- Muster & Vorlagen
- Dateiverwaltung zur Datenschutzdokumentation
- Datenexport (z.B. PDF)
- Kein Risiko, monatlich kündbar

Mit dem Absenden einer Bestellung über unsere Online-Plattform durch Anklicken des Buttons "PAKET JETZT BUCHEN" nach Auswahl des Pakets PLATTFORM gibt der Kunde eine rechtsverbindliche Bestellung ab. Der Vertrag kommt mit unserer Annahmeerklärung per E-Mail zustande. Wir können die Annahme auch durch Freischaltung des Pakets PLATTFORM erklären.

c) Darüber hinaus haben registrierte Kunden die Möglichkeit, einen unserer Experten als externen Datenschutzbeauftragten mit folgenden Leistungen zu bestellen („FULL-SERVICE“):

- Nutzung der Online-Plattform
- Software zur Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten
- Muster & Vorlagen
- Dateiverwaltung zur Datenschutzdokumentation
- Datenexport (z.B. PDF)
- Bestellung eines externen Datenschutzbeauftragten
- Erfüllung der gesetzlichen Aufgaben eines Datenschutzbeauftragten (Art. 39 DSGVO)
- Individuelle Hilfestellung bei der Erstellung der benötigten Datenschutz-Dokumentation

Mit dem Absenden einer Bestellung über unsere Online-Plattform durch Anklicken des Buttons "PAKET JETZT BUCHEN" nach Auswahl des Pakets FULL-SERVICE gibt der Kunde eine Anfrage zum Abschluss eines individuellen Vertrages ab. Wir werden uns anschließend bei dem Kunden melden und die Modalitäten eines zu schließenden Vertrages individuell abstimmen. Der Vertragsschluss kann sodann per E-Mail erfolgen.

(3) Wir speichern den Vertragstext nach Vertragsschluss nicht. Wir senden Ihnen jedoch den Vertragstext einschließlich dieser AGB per E-Mail zu.

(4) Der Vertragsschluss erfolgt in deutscher Sprache.

4. Pflichten des Kunden

(1) Der Kunde ist verpflichtet, im Registrierungsvorgang und bei Angabe der Firmendaten wahrheitsgemäße und vollständige Angaben zu machen und seine Daten stets auf dem aktuellen Stand zu halten. Mindestangaben für die Registrierung und die Erstellung eines Accounts sind die E-Mailadresse und ein Passwort. Bei Bestellung eines kostenpflichtigen Angebots sind weitere Angaben wie Firma, Name des Ansprechpartners, Anschrift und Kontaktdaten, erforderlich.

(2) Der Kunde verpflichtet sich, seine Zugangsdaten und insbesondere das Passwort vertraulich zu behandeln und diese unberechtigten Dritten gegenüber nicht offenzulegen. Erlangt der Kunde Kenntnis über den Missbrauch von Zugangsdaten oder Passwörtern, wird unverzüglich der Missbrauch unterbunden und wir werden informiert. Bei Missbrauch sind wir berechtigt, den Zugang zu sperren. Der Kunde haftet für einen von ihm zu vertretenden Missbrauch.

(3) Der Kunde verpflichtet sich ausdrücklich, die Rechercheergebnisse nur für den eigenen Gebrauch zu verwenden und nicht an Dritte weiterzugeben.

(4) Es ist dem Kunden untersagt, das über unser Online-Angebot zur Verfügung gestellte Datenmaterial zu vervielfältigen, zu verbreiten, öffentlich wiederzugeben, umzugestalten oder zum Verkauf anzubieten.

(5) Der Kunde hat selbst die für die Nutzung den Online-Angebots erforderlichen technischen Voraussetzungen zu schaffen. Er ist für die Beschaffung und den Unterhalt der benötigten Hardware sowie für die Anschlüsse an die öffentlichen Telekommunikationsnetze vom eigenen Endgerät zu dem Online-Angebot über das Internet selbst verantwortlich. Er trägt die anfallenden Telekommunikationskosten seines Telekommunikationsanbieters.

5. Widerrufsrecht

(1) Wenn der Kunde Verbraucher ist (siehe Ziffer 1 (2)), steht ihm nach Maßgabe der gesetzlichen Bestimmungen ein Widerrufsrecht zu.

(2) Es gelten die Regelungen der folgenden Widerrufsbelehrung:

Widerrufsbelehrung

Widerrufsrecht

Sie haben das Recht, binnen vierzehn Tagen ohne Angabe von Gründen diesen Vertrag zu widerrufen.

Die Widerrufsfrist beträgt vierzehn Tage ab dem Tag des Vertragsabschlusses.

Um Ihr Widerrufsrecht auszuüben, müssen Sie uns (DSGrundversorgung GmbH, Ericusspitze 4, 20457 Hamburg, Telefon: 040 / 33 46 18 69-0, E-Mail info@datenschutz-grundversorgung.de) mittels einer eindeutigen Erklärung (z.B. ein mit der Post versandter Brief, Telefax oder E-Mail) über Ihren Entschluss, diesen Vertrag zu widerrufen, informieren. Sie können dafür das folgende Muster-Widerrufsformular verwenden, das jedoch nicht vorgeschrieben ist.

Zur Wahrung der Widerrufsfrist reicht es aus, dass Sie die Mitteilung über die Ausübung des Widerrufsrechts vor Ablauf der Widerrufsfrist absenden.

Folgen des Widerrufs

Wenn Sie diesen Vertrag widerrufen, haben wir Ihnen alle Zahlungen, die wir von Ihnen erhalten haben, einschließlich der Lieferkosten (mit Ausnahme der zusätzlichen Kosten, die sich daraus ergeben, dass Sie eine andere Art der Lieferung als die von uns angebotene, günstigste Standardlieferung gewählt haben), unverzüglich und spätestens binnen vierzehn Tagen ab dem Tag zurückzuzahlen, an dem die Mitteilung über Ihren Widerruf dieses Vertrags bei uns eingegangen ist. Für diese Rückzahlung verwenden wir dasselbe Zahlungsmittel, das Sie bei der ursprünglichen Transaktion eingesetzt haben, es sei denn, mit Ihnen wurde ausdrücklich etwas anderes vereinbart; in keinem Fall werden Ihnen wegen dieser Rückzahlung Entgelte berechnet.

Muster-Widerrufsformular

(Wenn Sie den Vertrag widerrufen wollen, dann füllen Sie bitte dieses Formular aus und senden Sie es zurück.)

- An
DSGrundversorgung GmbH
Ericusspitze 4
20457 Hamburg

E-Mail: info@datenschutz-grundversorgung.de

- Hiermit widerrufe(n) ich/wir (*) den von mir/uns (*) abgeschlossenen Vertrag über den Kauf der folgenden Waren (*)/ die Erbringung der folgenden Dienstleistung (*)

- Bestellt am (*)/erhalten am (*)

- Name des/der Verbraucher(s)

- Anschrift des/der Verbraucher(s)

- Unterschrift des/der Verbraucher(s) (nur bei Mitteilung auf Papier)

- Datum

(*) Unzutreffendes streichen.

6. Nutzungs- und Urheberrechte

(1) Die in unserem Online-Angebot zur Verfügung gestellten Daten, Dokumente, Grafiken und sonstigen Inhalte unterliegen dem Urheberrecht. Wir erteilen dem Kunden das nicht ausschließliche, nicht übertragbare und nicht unterlizenzierbare, auf die Vertragsdauer befristete Recht an den zur Verfügung gestellten und abgespeicherten Dokumenten. Das Nutzungsrecht umfasst die Befugnis, den Inhalt der jeweiligen aufgerufenen Dokumente auf dem Bildschirm sichtbar zu machen und für die eigene Nutzung zu speichern sowie die Daten des Verzeichnisses von Verarbeitungstätigkeiten als PDF-Datei („PLATTFORM“ und "FULL-SERVICE") zu speichern. Eine darüberhinausgehende Nutzung, insbesondere eine Vervielfältigung, ist dem Kunden nur für den eigenen Gebrauch gestattet.

(2) Dem Kunden ist es insbesondere nicht gestattet, die in dem Online-Angebot erhaltenen Datenbestände in elektronischer oder anderer Form an Dritte zu veräußern oder weiterzugeben.

(3) Die nicht autorisierte Nutzung dieser Dokumente oder sonstiger urheberrechtlich geschützter Materialien ist ausdrücklich verboten und stellt eine Verletzung der Urheberrechte oder sonstiger Schutzrechte von uns dar.

7. Haftung

(1) Wir haben bei der Erstellung und Pflege des Online-Angebots größtmögliche Sorgfalt aufgewendet. Wir übernehmen keine Haftung für kurze Störungen der Erreichbarkeit des Online-Angebots, soweit diese nicht auf vorsätzlichem oder grob fahrlässigem Verhalten unsererseits oder unserer Erfüllungsgehilfen beruhen, insbesondere wenn die Ursache von Störungen nicht in unserem Einflussbereich liegt. Hierunter fallen u. a. Funktionsstörungen der Datenleitungen zum Server, auf dem sich das Online-Angebot befindet, sowie Strom- und Serverausfälle.

(2) Wir haften bei Vorsatz oder grober Fahrlässigkeit unbeschränkt.

(3) Im Falle leichter Fahrlässigkeit haften wir oder unsere Erfüllungsgehilfen nur bei der Verletzung solcher Pflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der Kunde regelmäßig vertraut und vertrauen darf (vertragswesentliche Pflichten oder Kardinalpflichten genannt), jedoch begrenzt auf den nach der Art der Leistung vorhersehbaren, vertragstypischen Schaden. Die Haftung ist für den Regelfall der Höhe nach beschränkt auf den Betrag eines Jahresnutzungsentgelts des von dem Kunden ausgewählten Pakets. Der Nachweis eines höheren Schadens bleibt dem Kunden vorbehalten.

(4) Die vorgenannten Haftungsbegrenzungen gelten nicht bei Arglist, im Falle von Körper- bzw. Personenschaden, für die Verletzung von Garantien sowie für Ansprüche aus dem Produkthaftungsgesetz.

8. Vertragslaufzeit / Kündigung

(1) Die Nutzung des Online-Angebots ist mit folgenden Vertragslaufzeiten möglich:

a) Der Vertrag über die Nutzung des Pakets „BASIS“ hat eine Laufzeit von 90 Tagen und endet mit Ablauf der Vertragslaufzeit automatisch. Der Zugriff auf die Inhalte ist nach Ablauf der Vertragslaufzeit nicht mehr möglich. Eine ordentliche Kündigung ist für beide Vertragsparteien innerhalb der Vertragslaufzeit ausgeschlossen.

b) Der Vertrag über die Nutzung des Pakets „PLATTFORM“ läuft auf unbestimmte Zeit und kann von dem Kunden ohne Einhaltung einer Frist jeweils zum Monatsende gekündigt werden. Wir sind berechtigt, den Vertrag jeweils mit einer Frist von drei Monaten zum Ende eines Kalenderjahres zu kündigen. Der Zugriff auf die Inhalte ist nach einer Kündigung durch den Kunden nach Ablauf der Vertragslaufzeit nicht mehr möglich. Erklären wir eine ordentliche Kündigung, werden wir dem Kunden die von ihm eingepflegten Inhalte und bearbeiteten Dokumente nach Ablauf der Vertragslaufzeit zur Verfügung stellen.

c) Der Vertrag über die Nutzung des Pakets „FULL-SERVICE“ hat eine Mindestlaufzeit von zwei Jahren. Er verlängert sich anschließend um jeweils ein weiteres Jahr, wenn er nicht von einer der Parteien mit einer Frist von drei Monaten gekündigt wird. Mit Beendigung des Vertrages endet die Bestellung zum externen Datenschutzbeauftragten. Weitere Details sind dem gesondert zu schließenden Dienstvertrag zur Bestellung eines externen Datenschutzbeauftragten zu entnehmen.

(2) Das Recht beider Parteien zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Für uns liegt ein außerordentlicher Kündigungsgrund insbesondere dann vor, wenn der Kunde bei der Registrierung, im Bestellvorgang oder späteren Änderung seiner Daten vorsätzlich fehlerhafte Angaben macht oder gegen diese AGB trotz einer vorherigen Abmahnung wiederholt verstößt.

(3) Die Kündigung bedarf der Textform (z.B. schriftlich oder per E-Mail an info@datenschutz-grundversorgung.de).

9. Gebühren und Zahlungsmodalitäten

(1) Der Kunde ist verpflichtet, die vereinbarten Gebühren zu zahlen. Die Höhe der Gebühren ist im Bestellvorgang ausgewiesen und versteht sich zuzüglich der gesetzlichen Umsatzsteuer.

(2) Wir werden die Gebühren jeweils am Anfang eines jeden Monats im Voraus in Rechnung stellen, erstmals ab dem 1. des auf den Vertragsschluss folgenden Monats. Die Vergütung ist innerhalb von 14 Tagen nach Rechnungsstellung fällig und ohne Abzug zahlbar. Auf Wunsch des Kunden werden wir die monatliche Vergütung mit einer Dauerrechnung abrechnen. Der Kunde kann den Wunsch per E-Mail an info@datenschutz-grundversorgung.de erklären.

10. Datenschutz und Geheimhaltung

(1) Die Parteien werden die jeweils anwendbaren gesetzlichen Datenschutzbestimmungen beachten und ihre im Zusammenhang mit dem Vertrag eingesetzten Beschäftigten auf Vertraulichkeit verpflichten, soweit diese nicht bereits allgemein entsprechend verpflichtet sind. Das Muster einer entsprechenden Verpflichtungserklärung kann der Kunde in unserer Online-Plattform im Bereich Vorlagen abrufen.

(2) Beide Parteien sind sich darüber einig, dass die Nutzung der Online-Plattform als Auftragsverarbeitung im Sinne des Art. 28 DSGVO anzusehen ist, bei der der Kunde aus datenschutzrechtlicher Sicht Verantwortlicher für die von ihm eingegebenen Daten bleibt. Vor diesem Hintergrund wird mit der Registrierung der als **Anlage** zu diesen AGB beigefügte Vertrag zur Auftragsverarbeitung geschlossen. Der Vertrag kommt mit dem Klick auf den Button „REGISTRIEREN >>“ zustande.

(3) Über die datenschutzrechtlichen Pflichten hinaus verpflichten sich beide Parteien, sämtliche Informationen und Daten, die ihnen im Zuge der Zusammenarbeit bekannt gegeben werden oder sonst bekannt werden, geheim zu halten, insbesondere nicht an Dritte weiterzugeben und nur im Rahmen der Zusammenarbeit zu nutzen. Von dieser Geheimhaltungsverpflichtung sind auch sämtliche Informationen und Daten erfasst, die unmittelbar oder mittelbar das dem Kunden zur Verfügung gestellte Online-Portal und dessen Funktionen betreffen und die nicht allgemein, sondern nur passwortgeschützt zugänglich sind. Die Geheimhaltungsverpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

11. Schlussbestimmungen

(1) Auf Verträge zwischen dem Anbieter und den Kunden findet das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts Anwendung. Die gesetzlichen Vorschriften zur Beschränkung der Rechtswahl und zur Anwendbarkeit zwingender Vorschriften insbes. des Staates, in dem der Kunde als Verbraucher seinen gewöhnlichen Aufenthalt hat, bleiben unberührt. Für Kunde, die keine Verbraucher sind oder die keinen ordentlichen Gerichtsstand in Deutschland haben, ist der Gerichtsstand für alle Streitigkeiten, die durch oder in Verbindung mit diesen AGB entstehen, Hamburg (Deutschland).

(2) Sollte eine Bestimmung dieser AGB unwirksam oder undurchführbar sein oder werden, so berührt dies die Wirksamkeit der übrigen Bestimmungen nicht. Die Vertragsparteien verpflichten sich vielmehr in einem solchen Fall anstelle der unwirksamen oder undurchführbaren Bestimmung eine wirksame oder durchführbare Bestimmung einzufügen, welche den wirtschaftlichen und ideellen Vorstellungen der Parteien am nächsten kommt.

(3) Streitbeilegung: Die EU-Kommission hat eine Internetplattform zur Online-Beilegung von Streitigkeiten geschaffen. Die Plattform dient als Anlaufstelle zur außergerichtlichen Beilegung von Streitigkeiten betreffend vertragliche Verpflichtungen aus Online-Verträgen. Nähere Informationen sind unter dem folgenden Link verfügbar: <https://ec.europa.eu/consumers/odr>. Zur Teilnahme an einem Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle sind wir weder bereit noch verpflichtet.

Anlage:

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

zwischen

dem auf der Online-Plattform <https://datenschutz-grundversorgung.de> registrierten Kunden
(siehe Ziffer 3 der AGB)

- nachfolgend „Auftraggeber“ genannt -

und der

DSGrundversorgung GmbH
Ericusspitze 4
20457 Hamburg

- nachfolgend „Auftragnehmer“ genannt –

1. Vertragsgegenstand und Dauer des Auftrags

(1) Grund für die Beauftragung ist die Nutzung des Online-Angebots des Auftragnehmers (<https://datenschutz-grundversorgung.de>) durch den Kunden (nachfolgend „Hauptvertrag“ genannt). Die Zusammenarbeit der Parteien nach diesem Hauptvertrag bringt es mit sich, dass der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers (nachfolgend „Auftraggeber-Daten“ genannt) erhält und diese ausschließlich im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 4 Nr. 8 DSGVO verarbeitet.

(2) Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Hauptvertrages und ersetzt einen eventuell bereits bestehenden Vertrag über die Verarbeitung personenbezogener Daten im Auftrag.

(3) Die Dauer dieses Vertrages richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrages (siehe Ziffer 8 der AGB). Eine isolierte Kündigung dieses Vertrages ist ausgeschlossen.

(4) Unbeschadet des vorstehenden Absatzes gilt der Vertrag so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).

2. Art und Zweck der vorgesehenen Verarbeitung von Daten

(1) Der Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ist in den AGB konkret beschrieben. Der Auftraggeber nutzt die von dem Auftragnehmer zur Verfügung gestellte Online-Plattform, um seine Datenschutzerklärungen und insbesondere das Verzeichnis von Verarbeitungstätigkeiten zu führen. Hierbei fallen personenbezogene Daten an und es werden von dem Auftraggeber auch personenbezogene Daten in die Online-Plattform eingepflegt.

(2) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten

- Planungs- und Steuerungsdaten
- Sämtliche personenbezogenen Daten, die der Auftraggeber zur Erstellung der Datenschutzdokumentation in die Online-Plattform einpflegt.

(3) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden
- Interessenten
- Beschäftigte
- Lieferanten
- Handelsvertreter
- Ansprechpartner

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technisch-organisatorische Maßnahmen gem. Art. 32 DSGVO zum Schutz der personenbezogenen Daten und übergibt dem Auftraggeber die Dokumentation zur Prüfung [**Anlage 1**]. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Vertrags.

(2) Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(3) Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer zukünftig gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Über wesentliche Änderungen, die durch den Auftragnehmer zu dokumentieren sind, ist der Auftraggeber unverzüglich in Kenntnis zu setzen.

4. Rechte von betroffenen Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Der Auftraggeber kann Weisungen insbesondere über die Online-Plattform selbst erteilen, indem er die Daten im Verzeichnis von Verarbeitungstätigkeiten oder Dokumente der Datenschutzdokumentation z.B. berichtigt oder löscht. Der Auftraggeber hat somit stets die Möglichkeit, auf die Verarbeitung der personenbezogenen Daten durch den Auftragnehmer direkten Einfluss zu nehmen.

(3) Soweit vom Leistungsumfang umfasst, sind die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat, zusätzlich zu der Einhaltung der Regelungen dieses Vertrags, eigene gesetzliche Pflichten gemäß der DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- Die Wahrung der Vertraulichkeit gemäß Artt. 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 berechtigterweise Zugang zu 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.

- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Vertrag 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.
- Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten, einem anderen Anspruch oder einem Informationersuchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- 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.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrags.
- Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Artt. 33, 34 DSGVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.
- Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung.
- Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

(2) Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DSGVO.

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 in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. 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 zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

(3) Der Auftraggeber stimmt der Beauftragung der folgenden Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO mit dem Unterauftragnehmer zu.

- soft-park Services GmbH, Holländischer Brook 2, 20457 Hamburg; technischer Betrieb, Weiterentwicklung, Wartung und Pflege der Online-Plattform, technischer Support
- beck Service GmbH, Ericusspitze 4, 20457 Hamburg; fachlicher Support (Datenschutz), Stellung von externen Datenschutzbeauftragten (Paket „FULL-SERVICE“)

Die vertragliche Vereinbarung wird dem Auftraggeber auf dessen Verlangen vorgelegt, wobei geschäftliche Klauseln ohne datenschutzrechtlichen Bezug hiervon ausgenommen sind.

Die Auslagerung auf andere Unterauftragnehmer oder der Wechsel der gemäß Absatz 3 bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit, die 14 Tage nicht unterschreiten darf, 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.

(4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

(5) 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.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht gestattet.

7. Internationale Datentransfers

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.

8. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen 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 während der üblichen Geschäftszeiten 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 der technisch-organisatorischen Maßnahmen zur Einhaltung der besonderen Anforderungen des Datenschutzes allgemein sowie solche, die den Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

9. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu

einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Die anfänglichen Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt.

(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 so lange 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 Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens aber mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Anlage 1:

Technische und organisatorische Maßnahmen beim Auftragnehmer

Die nachfolgenden Kategorien von Maßnahmen folgen den Vorgaben des Art. 32 DSGVO. Der Auftragnehmer wird mindestens die nachfolgend angeführten technischen und organisatorischen Maßnahmen erfüllen:

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

Zutrittskontrolle

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

- Sicherheitsschlösser und Chipkarten
- Zutrittsmittelverwaltung und Zutrittsmitteldokumentation: Dokumentation der Schlüsselvergabe, Schlüsselverzeichnis
- Zutrittsberechtigungskonzept
- Klingelanlage mit Video-/Sprechfunktion
- Fenster einbruchsicher (1.OG, vorgelagerte doppelte Verglasung)
- Aufenthalt von Besuchern nur in Anwesenheit von Mitarbeitern
- Sorgfältige Auswahl von Reinigungspersonal

Zugangskontrolle

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

- Zuordnung von Benutzerrechten in jedem System
- Identifizierung und Authentifizierung durch Benutzername/Passwort
- Passwort-Richtlinie: Jeder Account ist mit einem individuellen Passwort geschützt, es erfolgt keine Weitergabe von Passwörtern; Komplexität: „4 aus 4“ (Großbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen)
- Begrenzung der Fehlversuche
- Protokollierung und Auswertung der Zugriffe
- Arbeitsanweisung: Sperren des Bildschirms, Clean Desk Policy
- Einsatz von Anti-Viren-Software: Von Mitarbeitern genutzte PCs werden standardmäßig mit Anti-Viren-Software ausgestattet
- Einsatz einer Hardware-Firewall
- Einsatz von Software-Firewalls

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.)

- Berechtigungskonzept
- Verschlüsselung gespeicherter Personendaten
- Administratorenkonzept
 - Protokollierung der Administratortätigkeit und Auswertung der Protokolle
 - Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Berechtigungskonzept mit Rollen und unterschiedlichen Berechtigungsstufen (Geschäftsführung, Personal, Buchhaltung, IT etc.). Verwaltung der Rechte durch internen Systemadministrator: E-Mail-Adressen und Accounts werden ausschließlich vom Systemadministrator angelegt und archiviert (z.B. bei Ausscheiden eines Mitarbeiters)
- Sicheres Löschen von Datenträgern vor Wiederverwendung
- Ordnungsgemäße Datenträgervernichtung mit Protokollierung (DIN 66399)
- Vernichtung von Papier mit Aktenvernichter Sicherheitsstufe P5
- Verschlüsselung von Datenträgern (insbesondere Festplatten von Laptops)

Trennungsgebot

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

- Abschottung personenbezogener Daten: organisatorische Trennung
- Mehrere voneinander physische Systeme zum Verarbeiten von Daten
- Mehrere voneinander getrennte virtuelle Systeme zum Verarbeiten von Daten
- Logische Mandantentrennung (softwareseitig) für Nutzer-Accounts per User-ID
- Unterschiedliche Datenbanken
- Daten werden räumlich getrennt gesichert (automated Snapshots von Serversystemen)
- Trennung von Produktiv- und Testsystem
- Physikalische Trennung der Personaldaten (Papierform), Verwaltung von digitalen Personaldaten gemäß dem Berechtigungskonzept

Pseudonymisierung

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

- Trennung der Zuordnungsdaten und Aufbewahrung in einem getrennten und abgesicherten System
- Interne Anweisung zur Anonymisierung/Pseudonymisierung von personenbezogenen Daten im Falle einer Weitergabe

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

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.)

- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- Verschlüsselung der übertragenen Daten (Verfahren: SSL/TLS (HTTPS))
- Protokollierung von Übertragungen und monatliche Auswertung der Protokolle
- Verschlüsselung besonders sensibler Datenbankfelder
- Firewall: Backend ist nur auf definierten Ports geöffnet
- Sichere Aufbewahrung von Datenträgern, es erfolgt keine Weitergabe von Datenträgern an Dritte

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.)

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Auswertung und Aufbewahrung der Protokollierung
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können. (IT-Architekturbild)
- Nachvollziehbarkeit von Lesen, Eingabe, Änderung und Löschung von Daten im Rahmen des Berechtigungskonzeptes durch individuelle Benutzernamen (nicht Benutzergruppen)

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

Verfügbarkeitskontrolle

(Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.)

- Risiko- und Schwachstellenanalyse im Rahmen eines jährlichen Audits
- Datensicherung auf einem redundanten System
- alle 24h ein Backup in einen sicheren, ausgelagerten Ort
- Testen von Datenwiederherstellung
- Notfallplan Datenschutz
- Regelmäßige Schulung der Mitarbeiter bezüglich Sicherheitsanforderungen

- Serverraum nicht unter sanitärer Anlage
- Unterbrechungsfreie Stromversorgung (USV)
- Angriff von außen: Firewall und Anti-Virensoftware

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

- Automatische Backup-Funktion und Point-in-Time-Recovery
- Prüfung der Logdateien der Datensicherung und der Sicherungsmedien
- Wiederherstellung der Daten und Protokollierung

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Auftragskontrolle

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

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Schriftliche Verträge zur Auftragsdatenverarbeitung liegen vor und werden jährlich auditiert
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- Auftragnehmer hat Datenschutzbeauftragten bestellt
- Kontrolle der Einhaltung beim Auftragnehmer und/oder Überprüfung Zertifikat(e)

Datenschutzmanagement

- Datenschutz- und Datensicherheitskontrollen
- Unternehmensrichtlinie Datenschutz
- Datenschutzzschulungen für Mitarbeiter
- Dokumentation Verfahren/Verzeichnisse von Verarbeitungstätigkeiten (Verantwortlicher/Auftragsverarbeiter) sind vorhanden, vollständig und aktuell
- Einhaltung Datengeheimnis, sämtliche Mitarbeitende sind auf Vertraulichkeit verpflichtet
- Jährliche Audits

Incident-Response-Management

(Unterstützung bei der Reaktion auf Sicherheitsverletzungen)

- Einsatz von Firewall und regelmäßige Aktualisierung
- Einsatz von Spamfilter und regelmäßige Aktualisierung
- Einsatz von Virens Scanner und regelmäßige Aktualisierung
- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen und Datenpannen
- Dokumentation von Sicherheitsvorfällen und Datenpannen
- Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

Datenschutzfreundliche Voreinstellungen

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

datenschutz

grundversorgung

- Einfache Ausübung der Rechte auf Widerruf, Widerspruch und Löschung personenbezogener Daten durch technische Maßnahmen