

PRIVACY AS A SERVICE

Wir machen Datenschutz genial einfach und raketenschnell.

Preise und Konditionen

Stand Juli/2021

Inhaltsverzeichnis

<i>Prüfung der Drittstaaten-Transfers auf Basis der Vorgaben der deutschen Aufsichtsbehörden.</i>	<i>2</i>
<i>Automatischer Consent-Manager für Ihre Webseite.....</i>	<i>3</i>
<i>Automatisierter Sicherheitsscan für Ihre Webseite</i>	<i>4</i>
<i>Datenschutzbetreuung als externe(r) TÜV-zertifizierter DSB.....</i>	<i>6</i>
<i>Einzelpreisliste</i>	<i>8</i>

Prüfung der Drittstaaten-Transfers auf Basis der Vorgaben der deutschen Aufsichtsbehörden.

1. Einmalige Prüfung externer Dienstleister oder Auftragsverarbeiter auf das Vorhandensein von Datentransfers in die USA oder anderer Drittländer. Ausführlicher Report zu den Bedingungen der Datentransfers inklusive möglicher Vorschläge, um einen Datentransfer rechtssicherer gestalten zu können.

Für einen Dienstleister
Ab 3 Dienstleister
Ab 5 Dienstleister

110,00 €* einmalig
90,00 €* einmalig pro DL
70,00 €* einmalig pro DL

2. Überwachung der Dienstleister (Wechsel der Standardvertragsklauseln, Rechtsgrundlagen, AGBs oder technischen Grundlagen)
Benachrichtigung bei relevanten Änderungen

20,00 €* pro DL / Monat

*Alle Preise verstehen sich rein netto zzgl. der gesetzlichen MwSt.

Warum Sie von unserem Service richtig profitieren?

Nach dem EuGH-Urteil vom letzten Jahr müssen Verantwortliche bei der Übermittlung von personenbezogenen Daten an Dienstleister darauf achten, dass die Daten nicht ohne ausreichende technisch-organisatorische Maßnahmen oder rechtliche Garantien in Drittländer übermittelt werden. Hierzu gehören insbesondere auch die USA, aus denen die meisten der genutzten Tools und Programme kommen.



Gerade die Marktmacht der amerikanischen Anbieter stellt europäische Verantwortliche vor große Probleme.

Die Aufsichtsbehörden verlangen von den Verantwortlichen, dass sie die genutzten Dienstleister auf problematische Datentransfers hin untersuchen und in konkreten Problemfällen aktiv werden.

Wir übernehmen für Sie diese Aufgabe sehr effizient, da wir jeden Dienstleister natürlich nur einmal anschreiben und im günstigsten Fall Ihnen die bereits vorliegenden Informationen direkt übergeben können.

Zudem überwachen wir auf Wunsch Ihre Dienstleister im weiteren Verlauf, um Ihnen Änderungen an AGB, Privacy Polycys und anderen relevanten Stellen mitteilen zu können. So bleiben Sie bei der Entwicklung auf dem Laufenden. Die Überwachung der Dienstleister ist ebenfalls interessant für den Wechsel auf die neuen Standardvertragsklauseln, der bis Ende 2022 vorgenommen sein muss. Auch hier kann Ihnen unser Monitoring helfen, etwaige Fristen nicht zu versäumen.

Automatischer Consent-Manager für Ihre Webseite

1. Monatliche DSGVO-Prüfung mit automatischer Erstellung einer Datenschutzerklärung
2. Consent-Manager. Erfordert die monatliche DSGVO-Prüfung. Auf der Basis der ermittelten Skripte und Cookies wird die DSE automatisch erstellt.

10,00 €* pro Webseite pro Monat

15,00 €* pro Webseite pro Monat

*Alle Preise verstehen sich rein netto zzgl. der gesetzlichen MwSt.

Allgemein

Der Consent Manager ermöglicht Ihnen die Einwilligung von Websitebesuchern DSGVO-konform einzuholen, sodass Sie die Daten Ihrer Nutzer verwenden dürfen.



Anpassbar

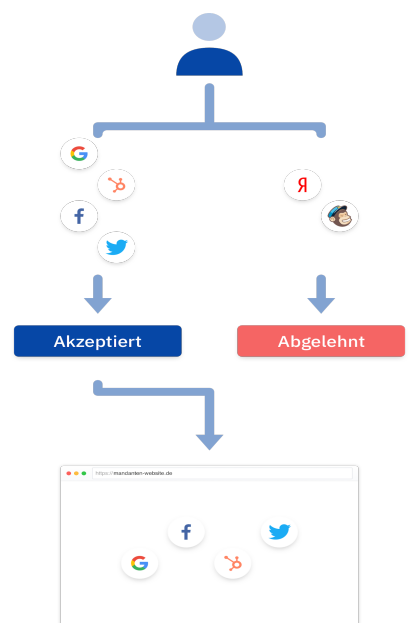
Die Farbgebung kann an Ihr Corporate Design angepasst werden. Die Schriftart wird von der Website übernommen. So gibt es keine Differenzen zu Ihrem aktuellen Webdesign.

Einwilligungsbanner

Sobald der Nutzer Ihre Website aufruft, wird ein benutzerfreundliches Fenster angezeigt. In diesem wird der Nutzer aufgeklärt und seine Einwilligung zur Datenverarbeitung erfragt. Der Nutzer kann jederzeit seine Einwilligung geben oder widerrufen. Das Tracking wird blockiert, bis der Nutzer seine Zustimmung erteilt hat.

Spracherkennung

Der Consent Manager ist in 13 Sprachen verfügbar. Zudem ist eine automatische Spracherkennung vorhanden, sodass die Sprache anhand der Browser-Einstellungen des Nutzers gewählt wird.

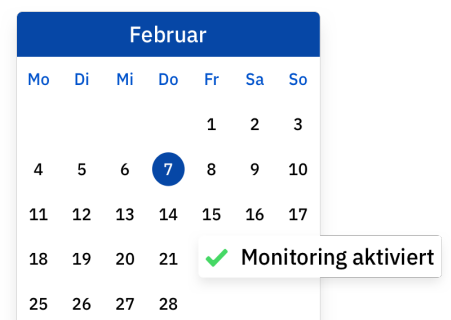


Immer auf dem neusten Stand

Ihre Website wird automatisch hinsichtlich DSGVO relevanten Kriterien gescannt. Dabei werden folgende Merkmale begutachtet:

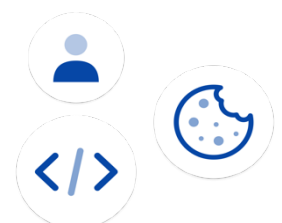
- Clientseitige-Anfragen, die beim Aufrufen Ihrer Website getätigt werden und nicht zu Ihrer Hauptdomain, oder einer Ihrer Subdomains führen.
- Gespeicherte Cookies beim bloßen Aufrufen Ihrer Website
- Vorhandensein und Status Ihres SSL-Zertifikates
- Standort Ihres Servers

Anhand der Überprüfung erkennt und listet der Consent Manager neu verwendete Drittanbieter und passt sich automatisch an. Sie brauchen keine manuelle Arbeit tätigen.



Einfache Umsetzung

Der Consent Manager ist plattformunabhängig und kann auf jeder Website verwendet werden. Die Implementierung kann Ihr Entwickler ganz einfach durch Kopieren einiger Zeilen Programmcode vornehmen.



Automatisierter Sicherheitsscan für Ihre Webseite

Sicherheitsscan für eine Webseite

285,00 €* pro Webseite

*Alle Preise verstehen sich rein netto zzgl. der gesetzlichen MwSt.

Wir führen einen Sicherheitscheck Ihrer Webseite durch. Dabei werden rund 400 verschiedene Angriffsszenarien durchgespielt. Sie erhalten anschließend einen ausführlichen Sicherheitsbericht.

Top 10 Sicherheitsrisiken für Webanwendungen

A1:2017-Injektion: Injektionsfehler, wie z. B. SQL-, NoSQL-, OS- und LDAP-Injektion, treten auf, wenn nicht vertrauenswürdige Daten als Teil eines Befehls oder einer Abfrage an einen Interpreter gesendet werden. Die feindlichen Daten des Angreifers können den Interpreter dazu verleiten, unbeabsichtigte Befehle auszuführen oder auf Daten ohne entsprechende Berechtigung zuzugreifen.

A2:2017-Broken Authentication: Anwendungsfunktionen im Zusammenhang mit der Authentifizierung und Sitzungsverwaltung sind oft fehlerhaft implementiert, sodass Angreifer Passwörter, Schlüssel oder Sitzungs-Tokens kompromittieren oder andere Implementierungsfehler ausnutzen können, um die Identität anderer Benutzer vorübergehend oder dauerhaft anzunehmen.

A3:2017 - Gefährdung sensibler Daten: Viele Webanwendungen und APIs schützen sensible Daten wie Finanz-, Gesundheits- und personenbezogene Daten nicht richtig. Angreifer können solche schwach geschützten Daten stehlen oder verändern, um Kreditkartenbetrug, Identitätsdiebstahl oder andere Straftaten durchzuführen. Sensible Daten können ohne zusätzlichen Schutz, wie z. B. Verschlüsselung im Ruhezustand oder bei der Übertragung, kompromittiert werden und erfordern besondere Vorsichtsmaßnahmen, wenn sie mit dem Browser ausgetauscht werden.

A4:2017-XML External Entities (XXE): Viele ältere oder schlecht konfigurierte XML-Prozessoren werten externe Entitätsreferenzen innerhalb von XML-Dokumenten aus. Externe Entitäten können verwendet werden, um interne Dateien über den Datei-URI-Handler, interne Dateifreigaben, internes Port-Scanning, Remote-Code-Ausführung und Denial-of-Service-Angriffe offenzulegen.

A5:2017-Broken Access Control: Beschränkungen dessen, was authentifizierte Benutzer tun dürfen, werden oft nicht richtig durchgesetzt. Angreifer können diese Schwachstellen ausnutzen, um auf nicht autorisierte Funktionen und/oder Daten zuzugreifen, z. B. auf Konten anderer Benutzer zuzugreifen, sensible Dateien anzuzeigen, Daten anderer Benutzer zu ändern, Zugriffsrechte zu ändern usw.

A6:2017-Security Misconfiguration: Sicherheitsfehlfunktion ist das am häufigsten auftretende Problem. Dies ist häufig eine Folge von unsicheren Standardkonfigurationen, unvollständigen oder Ad-hoc-Konfigurationen, offenen Cloud-Speichern, falsch konfigurierten HTTP-Headern und ausführlichen Fehlermeldungen, die sensible Informationen enthalten. Alle Betriebssysteme, Frameworks, Bibliotheken und Anwendungen müssen nicht nur sicher konfiguriert sein, sondern auch zeitnah gepatcht/aktualisiert werden.

A7:2017-Cross-Site Scripting XSS: XSS-Schwachstellen treten immer dann auf, wenn eine Anwendung nicht vertrauenswürdige Daten ohne ordnungsgemäße Validierung oder Escaping in eine neue Webseite einfügt oder eine bestehende Webseite mit vom Benutzer bereitgestellten Daten unter Verwendung einer Browser-API aktualisiert, die HTML oder JavaScript erstellen kann. XSS ermöglicht es Angreifern, Skripte im Browser des Opfers auszuführen, die Benutzersitzungen kapern, Websites umzustalten oder den Benutzer auf bösartige Websites umleiten können.

A8:2017-Unsichere Deserialisierung: Unsichere Deserialisierung führt häufig zu Remotecodeausführung. Selbst wenn Deserialisierungsfehler nicht zu Remote-Code-Ausführung führen, können sie für Angriffe wie Replay-Angriffe, Injection-Angriffe und Angriffe zur Privilegienweiterung genutzt werden.

A9:2017-Verwendung von Komponenten mit bekannten Sicherheitslücken: Komponenten, wie z. B. Bibliotheken, Frameworks und andere Softwaremodule, werden mit denselben Rechten wie die Anwendung ausgeführt. Wenn eine verwundbare Komponente ausgenutzt wird, kann ein solcher Angriff einen schwerwiegenden Datenverlust oder eine Serverübernahme ermöglichen. Anwendungen und APIs, die Komponenten mit bekannten Schwachstellen verwenden, können die Anwendungsabwehr untergraben und verschiedene Angriffe und Auswirkungen ermöglichen.

A10:2017 - Unzureichende Protokollierung und Überwachung: Unzureichende Protokollierung und Überwachung, gepaart mit fehlender oder ineffektiver Integration in die Incident Response, ermöglicht es Angreifern, weitere Systeme anzugreifen, die Persistenz aufrechtzuerhalten, auf weitere Systeme überzugehen und Daten zu manipulieren, zu extrahieren oder zu zerstören. Die meisten Studien zu Sicherheitsverletzungen zeigen, dass die Zeit bis zur Entdeckung einer Sicherheitsverletzung mehr als 200 Tage beträgt und in der Regel durch externe Parteien und nicht durch interne Prozesse oder Überwachung entdeckt wird.

Und hier sind alle Security-Checks im Überblick:

<ul style="list-style-type: none">• Eine Backdoor-Datei befindet sich auf dem Server• Umgehung der Zugangsbeschränkung durch Origin-Spoof• Erlaubte HTTP Methoden• Backup-Verzeichnis• Backup-Datei• Blinde NoSQL Injection (Differenzanalyse)• Blinde SQL Injection (Differenzanalyse)• Blinde SQL Injection (Zeitangriff)• CAPTCHA geschützte Form• Code-Injection• Code-Injection (php://input Wrapper)• Code-Injection (Zeitangriff)• Bekanntes Administrations-Interface• Bekanntes Verzeichnis	<ul style="list-style-type: none">• DOM-basiertes Cross-Site Scripting (XSS)• DOM-basiertes Cross-Site Scripting (XSS) im Script-Kontext• Offenlegung einer E-Mail-Adresse• Freigelegte localstart.asp Seite• Datei-Einschließung• Formularbasierter Datei-Upload• HTML Objekt• HTTP TRACE• HttpOnly Cookie• Unsicherer 'Access-Control-Allow-Origin' Header• Unsichere client-access policy• Unsicherer Cookie• Unsichere cross-domain policy (allow-access-from)• Unsichere cross-domain policy (allow-http-request-headers-from)
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

PRIVACY AS A SERVICE

Wir machen Datenschutz genial einfach und raketenschnell.

<ul style="list-style-type: none">• Bekannte sensible Datei• Cookie für übergeordnete Domain gesetzt• Bekanntgabe einer Kreditkartennummer• Cross-Site Request Forgery• Cross-Site Scripting (XSS)• Cross-Site Scripting (XSS) im Event-Tag eines HTML Elements• Cross-Site Scripting (XSS) im HTML-Tag• Cross-Site Scripting (XSS) im Pfad• Cross-Site Scripting (XSS) im Script-Kontext• CSRF• Offenlegung von CVS/SVN-Benutzern• Verzeichnis-Eintrag• Offenlegung von US-Sozialversicherungsnummer (SSN)• Unverschlüsseltes Passwort-Formular• Nicht überprüfte DOM-Weiterleitung• Nicht überprüfte Weiterleitung• WebDAV• XML External Entity• XPath Injection	<ul style="list-style-type: none">• Interessante Server-Antwort• LDAP Injection• Fehlkonfiguration in der LIMIT-Direktive der .htaccess-Datei• Fehlender 'Strict-Transport-Security' Header• Fehlender 'X-Frame-Options' Header• Gemischte Ressource• NoSQL Injection• Injektion von Betriebssystem-Befehlen• Injektion von Betriebssystem-Befehlen (Zeitangriff)• Passwortfeld mit Autovervollständigung• Pfadüberquerung• Offenlegung privater IP-Adressen• Öffentlich beschreibbares Verzeichnis• Remote File Inclusion• Response Splitting• Session fixation• Offenlegung des Quellcodes• SQL Injection
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Datenschutzbetreuung als externe(r) TÜV-zertifizierter DSB.

1. Initiale Bestandsaufnahme zu Beginn der Tätigkeit	
Size S	500,00 €* einmalig
Size M	950,00 €* einmalig
Size L	1.500,00 €* einmalig
Size XL	2.500,00 €* einmalig
Size XXL	3.500,00 €* einmalig
2. Monatliche Betreuung nach initialer Bestandsaufnahme	
Size S	220,00 €* p.M.
Size M	350,00 €* p.M.
Size L	550,00 €* p.M.
Size XL	850,00 €* p.M.
Size XXL	1.250,00 €* p.M.
3. Einzelne Beratungsstunde	150,00 €* pro Stunde

*Alle Preise verstehen sich rein netto zzgl. der gesetzlichen MwSt. Der Vertrag hat eine Laufzeit von 12 Monaten und verlängert sich um jeweils weitere 12 Monate, wenn er nicht mit Frist von 3 Monaten zum Ende der Laufzeit gekündigt wird. Die sinnvolle Paketgröße für Ihr Unternehmen wird in einem kostenlosen und unverbindlichen Orientierungsgespräch mit Ihnen abgestimmt.

Paket	Inklusive Standardleistung	Zusätzliche Leistungen nach Aufwand
Paket S Selbständige und Einzelunternehmer mit geringer und einfacher Verarbeitung personenbezogener Daten. (Handwerks- und Dienstleistungsbetriebe, die IT nur als Hilfsprozess nutzen)	<ul style="list-style-type: none"> • Musterdokumente je nach Branche • Entwurf eines branchenspezifischen VVT • Überprüfung von 2 AVV pro Jahr • 1 Tool-Prüfung (DSGVO-Konformität) • Überprüfung des Datenschutzstatus einmal pro Jahr • DSE für eine Webseite • Beratung 4 Stunden pro Jahr • Beratung per E-Mail jederzeit • Online-Schulungen für Mitarbeitende • Haftpflicht 250.000€ • Zertifizierter Datenschutzbeauftragter 	<ul style="list-style-type: none"> • Zusätzliche Beratungskontingente • Beratung zur DSFA • DSE für weitere Webseiten • Prüfung weiterer AVV • Consent-Manager • Security Check für Webseiten
Paket M Selbständige und Einzelunternehmer mit einer umfassenderen Bearbeitung personenbezogener Daten, z.B. durch Betrieb von Webshops oder anderen digitalen Geschäftsmodellen.	<ul style="list-style-type: none"> • Musterdokumente je nach Branche • Entwurf eines branchenspezifischen VVT • Überprüfung von 3 AVV pro Jahr • 2 Tool-Prüfungen (DSGVO-Konformität) • Überprüfung des Datenschutzstatus einmal pro Jahr • DSE für maximal 2 Webseiten • Beratung 6 Stunden pro Jahr • Beratung per E-Mail jederzeit • Online-Schulungen für Mitarbeitende • Haftpflicht 500.000€ • Bestellung als zertifizierter externer DSB 	<ul style="list-style-type: none"> • Zusätzliche Beratungskontingente • Beratung zur DSFA • DSE für weitere Webseiten • Prüfung weiterer AVV • Consent-Manager • Security Check für Webseiten • Ortsbegehung
Paket L Einzelunternehmen oder juristische Personen mit der Notwendigkeit, einen DSB zu benennen. Der Umfang der Verarbeitung der pb Daten entspricht dem eines mittleren Unternehmens. Hierunter fallen auch kleine IT-Dienstleister, die IT intern als Hilfsprozess nutzen)	<ul style="list-style-type: none"> • Musterdokumente je nach Branche • Entwurf eines branchenspezifischen VVT, • Pflege des VVT inklusive Einmeldung neuer Verfahren. • Überprüfung von 5 AVV pro Jahr • 4 Tool-Prüfungen (DSGVO-Konformität) • Überprüfung des Datenschutzstatus einmal pro Jahr • DSE für maximal 5 Webseiten • Beratung 10 Stunden pro Jahr • Beratung per E-Mail, jederzeit • Bestellung als zertifizierter externer DSB • Inklusiv ein Tochterunternehmen • Haftung 750.000 € • Support bei Datenschutzvorfällen innerhalb von 24 h 	<ul style="list-style-type: none"> • Zusätzliche Beratungskontingente • Beratung zu DSFA • DSE für weitere Webseiten • Prüfung weiterer AVV • Consent-Manager • Security Check für Webseiten • Ortsbegehung

PRIVACY AS A SERVICE

Wir machen Datenschutz genial einfach und raketenschnell.

Paket	Inklusive Standardleistung	Zusätzliche Leistungen nach Aufwand
Paket XL Einzelunternehmen oder juristische Personen mit umfangreichen Datenverarbeitungen oder angeschlossenen Tochterunternehmen. Hierunter fallen auch regionale IT-Dienstleister, die IT-Services anbieten, die das Verarbeiten personenbezogener Daten zum Inhalt haben, z.B. Webhoster, Shop-Anbieter, SaaS-Anbieter.	<ul style="list-style-type: none"> • Musterdokumente je nach Branche • Entwurf eines branchenspezifischen VVT, • Pflege des VVT inklusive Einmeldung neuer Verfahren. • Überprüfung von 11 AVV pro Jahr • 7 Tool-Prüfungen (DSGVO-Konformität) • Überprüfung des Datenschutzstatus einmal pro Jahr • DSE für maximal 5 Webseiten • Beratung 15 Stunden pro Jahr • Beratung per E-Mail, jederzeit • Beratung zu 1 DSFA pro Jahr • Bestellung als zertifizierter externer DSB • Inklusive 2 Tochterunternehmen • Haftung 1.000.000 € • Support bei Datenschutzvorfällen innerhalb von 24 h 	<ul style="list-style-type: none"> • Zusätzliche Beratungskontingente • Beratung zu weiteren DSFA • DSE für weitere Webseiten • Prüfung weiterer AVV • Consent-Manager • Security Check für Webseiten • Einbindung zusätzlicher Tochterunternehmen. • Ortsbegehung
Paket XXL Einzelunternehmen oder juristische Personen mit sehr umfangreichen oder komplexen Datenverarbeitungen oder mehreren angeschlossenen Tochterunternehmen. Hierunter fallen auch überregionale IT-Dienstleister mit einem umfangreichen Angebot an IT-Services, die das Verarbeiten personenbezogener Daten beinhalten.	<ul style="list-style-type: none"> • Musterdokumente je nach Branche • Entwurf eines branchenspezifischen VVT, • Pflege des VVT inklusive Einmeldung neuer Verfahren. • Überprüfung von 15 AVV pro Jahr • 10 Tool-Prüfungen (DSGVO-Konformität) • Überprüfung des Datenschutzstatus einmal pro Jahr • DSE für maximal 10 Webseiten • Beratung 20 Stunden pro Jahr • Beratung per E-Mail, jederzeit • Beratung zu 2 DSFA pro Jahr • Bestellung als zertifizierter externer DSB • Inklusive 3 weiteren Tochterunternehmen • Haftung 1.000.000 € • Support bei Datenschutzvorfällen innerhalb von 24 h 	<ul style="list-style-type: none"> • Zusätzliche Beratungskontingente • Beratung zu weiteren DSFA • DSE für weitere Webseiten • Prüfung weiterer AVV • Consent Manager • Security Check für Webseiten • Einbindung zusätzlicher Tochterunternehmen. • Ortsbegehung

Einzelpreisliste:

Einzeleistungen **

Entwurf eines branchenspezifischen VVT	200,00 €
Überprüfung eines AVV	300,00 €
Erste Überprüfung eines Auftragnehmers	450,00 €
Folgeprüfungen eines Auftragnehmers (alle 2 Jahre)	150,00 €
Erste Tool-Prüfungen (DSGVO-Konformität)	450,00 €
Folgeprüfungen eines Tools	150,00 €
DSE für eine Webseite	250,00 €
Folgeprüfung einer Webseite	150,00 €
Allgemeine Beratung (pro Stunde)	150,00 €
Beratungskontingente ab 5 Stunden (pro Stunde)	135,00 €
Jährliche Datenschutzprüfung	1.200,00 €
Auditierungen (zertifizierter Datenschutzauditor)	1.500,00 € pro Tag zzgl. Spesen
Reisekosten für Vor-Ort-Termine	nach Aufwand.

Monatliche Leistungen **

Pflege des VVT inklusive Einmeldung neuer Verfahren.	75,00 € pro Monat
Bestellung als zertifizierter externer DSB	180,00 € pro Monat.
Zusätzliches Tochterunternehmen	160,00 € pro Monat.

*Alle Preise verstehen sich rein netto zzgl. der gesetzlichen MwSt.

**Leistungen sind teilweise in den gebuchten Paketen bereits enthalten.