IGIT Information Technologies

Fenzlgasse 12 / 14 · 1150 Wien

phone +43 1 3530723
web igit.at
mail office@igit.at

IGIT Information Technologies

Fenzlgasse 12 / 14 · 1150 Wien

[Auftraggeber]

[Auftragsverarbeiter – im weiteren IGIT genannt]

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen o.a. Auftraggeber und IGIT wie folgt:

1. Allgemeines

1.1. IGIT verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Der Auftraggeber hat IGIT im Rahmen der Sorgfaltspflichten als Dienstleister ausgewählt. Voraussetzung für die Zulässigkeit einer Datenverarbeitung im Auftrag ist, dass der Auftraggeber IGIT den Auftrag schriftlich erteilt. Dieser Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den schriftlichen Auftrag zur Auftragsverarbeitung und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit dem Datenschutz.

1.2. Das Verarbeitungsverzeichnis nach Art. 30 DSGVO von IGIT ist wesentlicher Bestandteil der Auftragsverarbeitung und dokumentiert die vereinbarten Datenverarbeitungen und deren Änderungen, sowie die aktuell eingesetzten Auftragsverarbeiter, Datenkategorien, Rechtsgrundlagen, Aufbewahrungspflichten und TOMs (Technische und Organisatorische Maßnahmen). Änderungen werden dem Auftraggeber elektronisch zur Verfügung gestellt.

1.3. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung (nachfolgend „DSGVO“) zu verstehen.

2. Gegenstand des Auftrages

2.1. IGIT erbringt nach Abruf vom Auftraggeber unterschiedliche Leistungen im Bereich der Informationstechnologie. Für eine angemessene Dokumentation und Analyse der gesamten IT Netzwerkstruktur werden alle userspezifischen Daten (manuell oder durch Import aus dem Microsoft Windows Active Directory) und Assets im Netzwerk des Auftraggebers laufend inventarisiert, gescannt und – zum Teil automatisiert – von IGIT analysiert. Aufgrund des komplexen Gegenstandes ist insbesondere in sicherheitskritischen Ausnahmefällen die Durchführung von zusätzlichen Leistungen in Eigeninitiative von IGIT möglich.

2.2. Das IGIT Service Level Agreement (SLA, in früheren Versionen auch bezeichnet als Support Vereinbarung) ist Teil der Datenverarbeitung für den Auftraggeber und regelt im Wesentlichen:

» Reaktionszeiten
» Verfügbarkeit
» Art und Umfang der Dokumentation (Workplace- und Asset Management)
» Auftragserfassung (Ticketsystem IGIT, Mail)
» Inventarisierung und Analyse des IT Netzwerks
» Monitoring von unternehmenskritischen IT Assets
» Patch Management Clients / Server
» Umfang der Sicherungs-, Update und Virenschutzkontrolle

» Zusatzvereinbarungen in SLA:
» mtl. Maximalsumme (SLA und laufende Arbeiten)
» Rufbereitschaften

3. Dauer des Auftrags

3.1. Der Vertrag beginnt mit Unterzeichnung und wird auf unbestimmte Zeit geschlossen.

3.2. Er ist nur in Kombination mit dem Service Level Agreement (SLA) und unter dessen Bedingungen kündbar.

3.3. Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß von IGIT gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, IGIT eine Weisung des Auftraggebers bzgl. des Datenschutzes nicht ausführen kann oder will oder IGIT den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

4. Art und Zweck der Datenverarbeitung

Art und Zweck der Verarbeitung personenbezogener Daten durch IGIT für den Auftraggeber sind im Verarbeitungsverzeichnis von IGIT beschrieben.

5. Kategorien betroffener Personen

» Kunden (Auftraggeber)
» Interessenten
» Lieferanten
» Ansprechpartner
» Mitarbeiter/Beschäftigte (auch ehemalige Mitarbeiter/Beschäftigte)
» Bewerber

☐ _____
☐ _____
☐ _____
☐ _____

IGIT | Ing. Gratzl Information Technologies Fenzlgasse 12 | 14 1150 Wien UID: ATU61393058
Bank: Raiffeisenbezirksbank Güssing IBAN: AT613302700100706622 BIC: RLBBAT2E027

6. Art der personenbezogenen Daten

» Persönliche Identifikationsdaten
» Persönliche Detailangaben
» Öffentliche Identifikationsdaten
» Lebenslauf, Schulische Ausbildung
» Vertragsdaten
» Verrechnungsdaten
» Bonitätsdaten
» Clearing, Mahnwesen
» Finanzidentifikationsdaten (IBAN, BIC, …)
» Bestelldaten
» Entgeltdaten
» Anwesenheit und Disziplin
» Arbeitsorganisation
» Bildaufzeichnungen
» Tonaufzeichnungen
» Nutzung der Medien und Kommunikationsmittel
» Nutzung von EDV Mitteln
» Soziale Kontakte
» Unternehmenssicherheit (Passwörter, Zugangsdaten)
» Elektronische Zeiterfassung von Supporteinsätzen
» Userspezifische Problemstellungen

☐ _____
☐ _____
☐ _____
☐ _____
☐ _____
☐ _____
☐ _____
☐ _____
☐ _____
☐ _____
☐ _____
☐ _____

7. Rechte und Pflichten des Auftraggebers

7.1. Der Auftraggeber ist verantwortliche Stelle für die Verarbeitung von Daten im Auftrag durch IGIT. Die Beurteilung der Zulässigkeit der Datenverarbeitung obliegt allein dem Auftraggeber. IGIT steht das Recht zu, den Auftraggeber auf seiner Meinung nach rechtlich unzulässigen Datenverarbeitungen hinzuweisen.

7.2. Der Auftraggeber ist verantwortlich für die Wahrung der Betroffenenrechte. Betroffenenrechte sind gegenüber dem Auftraggeber wahrzunehmen. IGIT wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber IGIT geltend machen.

IGIT | Ing. Gratzl Information Technologies Fenzlgasse 12 | 14 1150 Wien UID: ATU61393058
Bank: Raiffeisenbezirksbank Güssing IBAN: AT613302700100706622 BIC: RLBBAT2E027

7.3. Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der bei IGIT getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit zu überzeugen. Der Auftraggeber wird das Ergebnis in geeigneter Weise dokumentieren.

7.4. Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber IGIT zu erteilen. Weisungen müssen schriftlich erfolgen.

7.5. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers bei IGIT entstehen, bleiben unberührt.

7.6. Der Auftraggeber kann weisungsberechtigte Personen benennen. Weisungsberechtigte Personen des Auftraggebers sind:

» Name: _____, Tel / Mail: _____

» Name: _____, Tel / Mail: _____

» Name: _____, Tel / Mail: _____

» Name: _____, Tel / Mail: _____

Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies IGIT schriftlich mitteilen.

7.7. Der Auftraggeber informiert IGIT unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch IGIT feststellt.

7.8. Für den Fall, dass eine Informationspflicht gegenüber Dritten besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

8. Allgemeine Pflichten von IGIT

8.1. IGIT verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen (entspr. diesem Vertrag, SLA, Verarbeitungsverzeichnis IGIT) und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach den genannten Vereinbarungen und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist IGIT untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

8.2. Vom Auftraggeber erhaltene und nicht mehr benötigte Kopien personenbezogener Daten und Dateien werden von IGIT datenschutzgerecht vernichtet.

8.3. IGIT ist verpflichtet, ihr Unternehmen und ihre Betriebsabläufe so zu gestalten, dass die Daten, die im Auftrag des Auftraggebers verarbeitet werden, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. IGIT wird den Auftraggeber über Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab informieren.

8.4. IGIT erklärt rechtsverbindlich, dass sie alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen

IGIT | Ing. Gratzl Information Technologies Fenzlgasse 12 | 14 1150 Wien UID: ATU61393058
Bank: Raiffeisenbezirksbank Güssing IBAN: AT613302700100706622 BIC: RLBBAT2E027

gesetzlichen Verschwiegenheitsverpflichtung gemäß §6 des Datenschutzanpassungsgesetzes 2018 unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung (NDA: „Non-disclosure-agreement“) der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

8.5. IGIT erklärt rechtsverbindlich, dass sie alle erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32ff DSGVO ergriffen hat. Konkret handelt es sich hierbei um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme.

8.6. IGIT wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. IGIT ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

8.7. Erhält IGIT einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat sie - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen.

8.8. IGIT ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers unverzüglich mitzuteilen, der im Zuge der Verarbeitung von Daten durch sie oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist. Ferner wird IGIT den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde gegenüber IGIT tätig wird und dies auch eine Kontrolle der Verarbeitung, die IGIT im Auftrag des Auftraggebers erbringt, betreffen kann.

8.9. Für den Fall, dass IGIT feststellt oder Tatsachen die Annahme begründen, dass von ihr für den Auftraggeber verarbeitete

- » besondere Arten personenbezogener Daten oder
- » personenbezogene Daten, die einem Berufsgeheimnis unterliegen oder
- » personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen oder
- » personenbezogene Daten zu Bank- oder Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, hat IGIT den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalls/der Vorfälle schriftlich zu informieren. Die Information muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung enthalten. Die Information soll zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung beinhalten. IGIT ist darüber hinaus verpflichtet, unverzüglich mitzuteilen, welche Maßnahmen durch IGIT getroffen wurden, um die unrechtmäßige Übermittlung bzw. unbefugte Kenntnisnahme durch Dritte künftig zu verhindern.

9. Ort der Durchführung der Datenverarbeitung

9.1. Um die vereinbarten SLA (Service Level Agreements, in früheren Versionen auch als Reaktionszeiten bezeichnet) einzuhalten, ist die Verarbeitung von personenbezogenen Daten im

Auftrag des Auftraggebers auch außerhalb der Betriebsstätten des Auftraggebers, von IGIT oder ihrer Auftragsverarbeitern zulässig.

9.2. Datenverarbeitungen werden zumindest zum Teil auch außerhalb der EU bzw. des EWR durchgeführt, und zwar derzeit in

» USA
» Schweiz
□ _____

Die aktuelle Liste der Drittländer und des angemessenen Datenschutzniveaus ist im Verarbeitungsverzeichnis von IGIT ersichtlich. Das angemessene Datenschutzniveau ergibt sich aus

» Einem Angemessenheitsbeschluss der Europäischen Kommission nach Art 45 DSGVO.
□ Einer Ausnahme für den bestimmten Fall nach Art 49 Abs 1 DSGVO.
□ Verbindlichen internen Datenschutzvorschriften nach Art 47 iVm Art 46 Abs 2 lit b DSGVO.
□ Standarddatenschutzklauseln nach Art 46 Abs 2 lit c und d DSGVO.
□ Genehmigten Verhaltensregeln nach Art 46 Abs 2 lit e iVm Art 40 DSGVO.
□ Einen genehmigten Zertifizierungsmechanismus nach Art 46 Abs 2 lit f iVm Art 42 DSGVO.
□ Von der Datenschutzbehörde bewilligte Vertragsklauseln nach Art 46 Abs 3 lit a DSGVO.
□ Einer Ausnahme für den Einzelfall nach Art 49 Abs 1 Unterabsatz 2 DSGVO.

10. Kontrollbefugnisse

10.1. Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch IGIT jederzeit im erforderlichen Umfang zu kontrollieren.

10.2. IGIT ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

10.3. Der Auftraggeber kann eine Einsichtnahme in die von IGIT für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

10.4. Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte von IGIT zu den jeweils üblichen Geschäftszeiten sowie nicht häufiger als alle 12 Monate vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe von IGIT durch die Kontrollen nicht unverhältnismäßig zu stören.

10.5. IGIT ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber, insbesondere im Hinblick auf Auskunfts- und Kontroll-pflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen von IGIT zu informieren.

10.6. Wenn IGIT in einem Unterauftragsverhältnis steht, so hat nicht nur der direkte Auftraggeber die oben genannten Kontrollbefugnisse, sondern auch der Hauptauftraggeber.

IGIT | Ing. Gratzl Information Technologies Fenzlgasse 12 | 14 1150 Wien UID: ATU61393058
Bank: Raiffeisenbezirksbank Güssing IBAN: AT613302700100706622 BIC: RLBBAT2E027

11. Unterauftragsverhältnisse

11.1. Die Beauftragung und/oder der Wechsel von Subunternehmen durch IGIT ist zulässig, soweit IGIT dies dem Auftraggeber eine angemessene Zeit vorab schriftlich anzeigt und der Auftraggeber nicht gegenüber IGIT schriftlich Einspruch gegen die geplante Auslagerung erhebt und die erforderlichen Vereinbarungen zwischen IGIT und dem Sub-Auftragsverarbeiter gemäß des Art. 28 Abs. 4 DSGVO abgeschlossen werden. Alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse sind im Verarbeitungsverzeichnis von IGIT ersichtlich.

11.2. IGIT hat den Subunternehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und IGIT getroffenen Vereinbarungen einhalten kann.

11.3. IGIT hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber den Subunternehmern gelten. IGIT hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.

11.4. IGIT hat mit dem Subunternehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen der DSGVO entspricht.

11.5. IGIT ist insbesondere verpflichtet, durch vertragliche Regelungen (Auftragsverarbeitungsvertrag) sicherzustellen, dass die Kontrollbefugnisse (Ziff. 10 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

11.6. Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 5 sind Dienstleistungen anzusehen, die IGIT bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die IGIT für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. IGIT ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Wartungs- und Prüfungsleistungen stellen zustimmungspflichtige Unterauftragsverhältnisse dar, soweit die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

12. Datengeheimnis

12.1. IGIT ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung des Datengeheimnisses im Sinne der DSGVO verpflichtet. IGIT verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, IGIT etwaige besondere Geheimnisschutzregeln mitzuteilen.

12.2. IGIT sichert zu, dass ihr die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und sie mit der Anwendung dieser vertraut ist. IGIT sichert ferner zu, dass sie die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und diese auf das Datengeheimnis i.S.d. DSGVO verpflichtet werden.

IGIT | Ing. Gratzl Information Technologies Fenzlgasse 12 | 14 1150 Wien UID: ATU61393058
Bank: Raiffeisenbezirksbank Güssing IBAN: AT613302700100706622 BIC: RLBBAT2E027

13. Wahrung von Betroffenenrechten

13.1. Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich.

13.2. Soweit eine Mitwirkung von IGIT für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird IGIT die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen.

13.3. IGIT unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation). Besonders zu beachten ist die Pflicht der unverzüglichen Mitteilung von Verletzungen des Schutzes personenbezogener Daten von IGIT an den Auftraggeber.

13.4. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber bei IGIT entstehen, bleiben unberührt.

14. Geheimhaltungspflichten

14.1. Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den vereinbarten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

14.2. Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

15. Vergütung

Die Vergütung von IGIT wird gesondert vereinbart.

16. Technische und organisatorische Maßnahmen zur Datensicherheit

16.1. IGIT verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind.

16.2. Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als „Anlage 1“ zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird IGIT im Vorwege mit dem Auftraggeber abstimmen. Maßnahmen, die

IGIT | Ing. Gratzl Information Technologies Fenzlgasse 12 | 14 1150 Wien UID: ATU61393058
Bank: Raiffeisenbezirksbank Güssing IBAN: AT613302700100706622 BIC: RLBBAT2E027

lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können von IGIT ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der von IGIT getroffenen technischen und organisatorischen Maßnahmen anfordern.

16.3. IGIT wird die von ihr getroffenen technische und organisatorische Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird IGIT den Auftraggeber informieren.

17. Beendigung

17.1. Nach Beendigung des Vertrages hat IGIT sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Gespeicherte Daten auf den Datenträgern von IGIT sind danach zu löschen.

17.2. IGIT ist verpflichtet, die Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.

17.3. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch IGIT entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Sie kann sie zu ihrer Entlastung bei Vertragsende dem Auftraggeber übergeben.

17.4. Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten bei IGIT zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte von IGIT erfolgen. Die Vor-Ort-Kontrolle muss mit angemessener Frist durch den Auftraggeber angekündigt werden.

18. Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch IGIT i.S.d. § 369 UGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

19. Schlussbestimmungen

19.1. Sollte das Eigentum des Auftraggebers bei IGIT durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat IGIT den Auftraggeber unverzüglich zu informieren. IGIT wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

19.2. Für Nebenabreden ist die Schriftform erforderlich.

19.3. Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

IGIT | Ing. Gratzl Information Technologies Fenzlgasse 12 | 14 1150 Wien UID: ATU61393058
Bank: Raiffeisenbezirksbank Güssing IBAN: AT613302700100706622 BIC: RLBBAT2E027

19.4. Dieser Vertrag wird in zwei Ausfertigungen erstellt, wobei der Auftraggeber und IGIT je eine Ausfertigung erhalten.

19.5. Erfüllungsort und Gerichtsstand ist Wien. IGIT ist jedoch berechtigt, den Vertragspartner an jedem anderen gesetzlichen Gerichtsstand zu verklagen.

Wien, am .... , am .....

....

Unterschrift Auftragsverarbeiter (IGIT) Unterschrift Auftraggeber

IGIT | Ing. Gratzl Information Technologies Fenzlgasse 12 | 14 1150 Wien UID: ATU61393058
Bank: Raiffeisenbezirksbank Güssing IBAN: AT613302700100706622 BIC: RLBBAT2E027

Anlage 1

Technische und organisatorische Maßnahmen von IGIT gemäß DSGVO

Auftragskontrolle

» Auswahl des Auftragsverarbeiters / Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
» Verpflichtung der Mitarbeiter von IGIT auf das Datengeheimnis

Eingabekontrolle

» Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
» D.h.: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Standard-Berechtigungsprofile auf „need to know-Basis“, Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten
» Aufzeichnung der Fernwartungssitzung beim Erhalt einer Fernwartung durch Drittanbieter (Auftragsverarbeiter)

Trennungsgebot

» Erstellung eines Berechtigungskonzepts. D.h.: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Standard-Berechtigungsprofile auf „need to know-Basis“, Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen
» Logische Mandantentrennung (softwareseitig)

Verfügbarkeitskontrolle

» Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
» Erstellen eines Backup- & Recovery Konzepts
» Feuer- und Rauchmeldeanlagen
» Klimaanlage in Serverräumen und für unternehmenskritische Assets
» Monitoring von unternehmenskritischen Assets, z.B. Firewalls, Server (Host und virtuelle Server), freie Festplattenkapazitäten, Backup -Speicherplatz und -Verfügbarkeit, Switches, WLANs
» Schutzsteckdosenleisten in Serverräumen
» Regelmäßige Tests der Datenwiederherstellung aus aktuellen Sicherungen
» Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
» Einsatz und richtige Dimensionierung Unterbrechungsfreie Stromversorgung (USV)

Weitergabekontrolle

IGIT | Ing. Gratzl Information Technologies Fenzlgasse 12 | 14 1150 Wien UID: ATU61393058
Bank: Raiffeisenbezirksbank Güssing IBAN: AT613302700100706622 BIC: RLBBAT2E027

» Einrichtungen von Standleitungen bzw. VPN-Tunneln

Zugangskontrolle

» Hardware, Firmware und Betriebssysteme am aktuellen Stand (speziell bei sicherheitsrelevanten Assets)
» Einsatz von Antiviren Software
» Sorgfältige Auswahl Mitarbeiter
» Authentifikation mit Benutzername / Passwort
» Gehäuseverriegelungen (z.B. Serverschrank, Server, Backuphardware)
» Einsatz einer Hardware Firewall
» Einsatz von Intrusion Detection Systemen
» Einsatz von Intrusion Prevention Systemen
» Schlüsselregelung (Schlüsselausgabe etc.)
» Sicherheitsschlösser
» Vergabe von temporären Passwörtern für Drittanbieter (temporäre Auftragsverarbeiter), die diese im Zuge der Wartung / Fernwartung eines Systems benötigen. Die Gültigkeitsdauer und Berechtigungen der Zugänge auf das nötigste beschränken.
» Verschlüsselung von Datenträgern in Laptops / Notebooks
» Einsatz von VPN Technologie
» Zugriffskontrolle
» Einsatz von geeigneten Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
» Arbeitsplätze werden nach 10 Minuten Inaktivität automatisch gesperrt
» Nach 10 falschen Eingabe der Zugangsdaten wird der Account automatisch (für 30 Minuten) gesperrt
» Erstellen eines Berechtigungskonzepts
» D.h.: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Standard-Berechtigungsprofile auf „need to know-Basis“, Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten
» Arbeitsplätze sind beim Verlassen zu sperren
» Beim Erhalt einer Fernwartung durch Drittanbieter (Auftragsverarbeiter), ist durch Schließen aller nicht erforderlichen Informationen, sowie Dokumenten und Anwendungen ein ungewollter Datenabfluss durch z.B. Screenshots zu vermeiden.
» physische Löschung von Datenträgern vor Wiederverwendung
» Verwaltung der Rechte durch Systemadministrator
» Notebooks, Tablets, Mobiltelefone usw. (mobile Assets) sind
» entweder in versperrten Räumlichkeiten aufzubewahren,
» beim Transport nicht unbeaufsichtigt / für betriebsfremde zugänglich bzw.
» bei kurzzeitiger Verwahrung im Fahrzeug, Fahrzeug verschlossen und Assets nicht sichtbar aufbewahrt.

Zutrittskontrolle

» Sorgfältige Auswahl Mitarbeiter
» protokollierte Schlüsselausgabe

IGIT | Ing. Gratzl Information Technologies Fenzlgasse 12 | 14 1150 Wien UID: ATU61393058
Bank: Raiffeisenbezirksbank Güssing IBAN: AT613302700100706622 BIC: RLBBAT2E027