AUP – Acceptable Use Policy (Weisung zur akzeptablen Nutzung)

I. AUP IT-ONBASE AG (nachfolgend ITOB genannt)

Diese AUP der ITOB gilt für die Nutzung aller von ITOB bereitgestellten Dienstleistungen und Produkte, unabhängig davon, ob ITOB diese direkt oder über eine Drittpartei für den Kunden bereitstellt. Die AUP regelt die Einhaltung der für alle IT-onBase-Dienste geltenden Gesetzte und Vorschriften. ITOB stellt den Kunden ihre Dienstleistungen nur zur Verfügung, wenn dieser vorgängig der AUP zugestimmt hat.

1. GENERELLE VERHALTENSREGELN

Nachfolgend beschrieben sind generelle Verhaltensregeln, die für den ordnungsmässigen Gebrauch aller Dienstleistungen der ITOB gelten.

Der Kunde verpflichtet sich dazu:

- die Dienstleistungen der ITOB in einer Wiese zu nutzen, damit der normale Betrieb, die Privatsphäre oder die Sicherheit fremden Eigentums (z.B. fremde Konten, Webseiten, Domainnamen, URLs, Netzwerke, Daten und sonstige Informationen) nicht beeinträchtigt wird;
- die Dienstleistungen der ITOB nur dazu zu verwenden;
- seine Zugangsdaten sicher aufzubewahren;
- seine Zugangsdaten nicht an Dritte (andere Mitarbeiter etc.) weitergibt;
- besonders schützenswerte Daten verschlüsselt zu versenden und abzulegen;
- bei eingehenden E-Mails zu prüfen, ob es sich um Phishing Mails handelt;
- den Versuch zu unterlassen, selbst oder Dritte dazu zu beauftragen, Informationen oder Daten von ITOB oder Dritten unbefugt abzurufen, in Datennetze von ITOB oder Dritten einzudringen oder in Programme, die von ITOB betrieben werden einzugreifen.

Dem Kunden von ITOB ist es insbesondere untersagt:

- die Dienste der ITOB zu missbrauchen;
- gesetzeswidrige und illegale, rassistische, pornografische, gegen das Menschenrecht verstossende Informationen, Daten oder sonstiges Material zu speichern, zu übertragen, zu versenden, zu verbreiten oder in Auftrag zu geben;
- andere zu einem Verhalten zu ermuntern, welches gegen nationales oder internationales Recht verstösst, eine strafbare oder ordnungswidrige Handlung begründet oder anderweitig gegen die öffentliche Sicherheit und Ordnung verstösst.
- die Privatsphäre Dritter zu verletzen oder gegen anderweitig geltende Gesetzte zu verstossen (z.B. die Datenschutz- und Persönlichkeitsrechte);
- ITOB Dienstleistungen dazu zu verwenden, fremdes Eigentum unbefugt zu überwachen oder auf fremdes Eigentum zu verweisen, ohne vorherige ausdrückliche Einwilligung des Eigentümers;
- die geistigen Eigentumsrechte Dritter zu verletzen;
- Musik, Videos, Software oder anderes durch geistiges Eigentum geschütztes Material ohne vorgängige Einholung der nötigen Einwilligungen zu veröffentlichen oder veröffentlichen zu lassen, hochzuladen oder anderweitig zu verbreiten;
- Dateien hochzuladen, die Viren, beschädigte Dateien oder irgendwelche Programme enthalten, welche die Funktionalität eines fremden Computers schädigen oder beeinträchtigen können;
- Dateien herunterzuladen unter dem Wissen, dass diese nicht rechtmässig in besagter Weise verbreitet werden dürfen;
- die Herkunft, Quelle von Software oder die in einer hochgeladenen Datei enthaltenen Daten zu fälschen oder zu löschen;
- zu verursachen, dass die Verwendung der IT-onBase-Dienstleistungen und Webseite für andere Benutzer eingeschränkt oder unterbunden wird;

Der Kunde verpflichtet sich, diese AUP einzuhalten und haftet für Verstösse.

ITOB überwacht die Einhaltung der AUP und behält sich das Recht vor, gesetzeswidrige Informationen, Daten oder sonstiges Material unverzüglich und ohne vorherige Ankündigung von ihren Servern oder aus ihren Diensten zu entfernen.

Wenn dem Kunden ein Verstoss gegen diese AUP bekannt ist oder er den Verdacht eines Verstosses gegen diese AUP hegt, ist er verpflichtet, ITOB unverzüglich schriftlich darüber in Kenntnis zu setzen.

Der Schutz der Privatsphäre ist ITOB sehr wichtig. Sie prüft E-Mails bzw. Daten ihrer Kunden nur, wenn dies, unter Wahrung der erforderlichen Sorgfalt, notwendig erscheint. Z.B. bei der Suche oder Beseitigung von Fehlern, bei Problemen bei der Zustellung von E-Mails oder wenn ITOB aufgrund gesetzlicher bzw. behördlicher Verfahren dazu verpflichtet ist.

Diese AUP wird in regelmässigen Abständen aktualisiert. Eine Aktualisierung wird dem Kunden durch die Veröffentlichung auf der ITOB Webseite mitgeteilt. Der Kunde verpflichtet sich, die AUP regelmässig zu lesen und diese immer einzuhalten.

2. Datenschutz und Datensicherheit

2.1. ITOB verwaltet die Daten der Kunden streng vertraulich. Die Daten werden ausschliesslich von Mitarbeitenden von IT-onBase oder ITOB Partnern verwendet. Die Kundendaten werden erfasst, um die Leistungen kontinuierlich zu verbessen und die vom Kunden bezogenen Dienstleistungen bereitzustellen und abzurechnen.

2.2. Daten können verwendet werden, um dem Kunden neue und verbesserte Dienstleistungen anbieten zu können.

2.3. Beide Parteien verpflichten sich zur Einhaltung der gesetzlichen Bestimmungen über den Datenschutz.

2.4. IT-onBase verpflichtet sich zur Einhaltung der Bestimmungen des Bundesgesetztes über den Datenschutz vom 19. Juni 1992.

2.5. Der Kunde trifft vor Ort geeignete Massnahmen um Datensicherheit und -schutz ausreichend zu gewährleisten. Insbesondere bestätigt der Kunde, dass die berechtigten Personen gem. AGB Art. 28.1 im Bereich des Datenschutzes entsprechend geschult sind und die nötige Sorgfalt bei der Erteilung jeglicher Aufträge an die ITOB wahren ohne explizit darauf aufmerksam gemacht zu werden. Die ITOB und deren Mitarbeitende gehen im guten Treu und Glauben davon aus, dass ausschliesslich Personen benannt werden, welche die nötigen Kompetenzen aufweisen."

2.6. ITOB ist besorgt, dass keine unberechtigten Zugriffe auf die Daten des Kunden möglich sind und schützt diese durch die erforderlichen Sicherheitsmassnahmen. Um die Risiken vor unbefugter Nutzung bestmöglich einzudämmen, werden diese laufend geprüft und angepasst

2.7. Der Kunde ist beim Versenden von Daten für die Datensicherheit selber verantwortlich. Eine E-Mail z.B. passiert während der Dauer des Versands, d.h. von Absender bis zum Empfänger, zahlreiche Internet-Mailserver. Keiner dieser Mailserver garantiert den Schutz der Privatsphäre, auch die Mailserver der ITOB nicht. Verlangt der Kunde absoluten Schutz der Privatsphäre muss er ein Verschlüsselungssystem verwenden. So sind die entsprechenden Mails nur für diejenigen lesbar, die im Besitz des richtigen Schlüssels sind.

3. System- und Netzsicherheit

3.1. Der Kunde unterlässt jeden Versuch, die Benutzer-Authentifikation bzw. die Sicherheit eines Hosts, eines Netzes oder Kontos zu umgehen ("Hacking" und "Cracking"). Darunter fallen u.a.

- der Zugriff auf nicht für den Kunden bestimmte Daten;
- Einloggen auf einem Server bzw. in ein Konto, für die dem Kunden seitens der ITOB keine ausdrückliche Zugangsberechtigung erteilt wurde;
- Testen der Sicherheit des IT-onBase-Netzes oder Netzwerke von ITOB Partnern bzw. anderer Netze (z.B. Betreiben eines Netzwerk-Scans o.ä.). Jeder Netzwerk-Scan oder Scan in ähnlicher Art wird als aktiver Hacking/Cracking-Versuch betrachtet.

3.2. Der Kunde unterlässt jeden Versuch, Dienstleistungen, welche für einen Anwender, Host oder Netz erbracht werden, zu stören ("Denial-of-Service"-Angriff). Hierunter fallen u.a.

- vorsätzliche Versuche, Dienste zu überlasten und Versuche, auf einem Host einen "Crash" herbeizuführen.

3.3. Der Kunde unterlässt jeden Versuch, Programme, Skripts oder Befehle zu verwenden oder Nachrichten zu senden, die die Computersitzung eines Anwenders durch irgendwelche Mittel bzw. über das Internet stören oder stören könnten.

4. Unbefugte Konten- oder Computernutzung

Der Kunde unterlässt es, ein Internet-/User-Konto oder einen Computer ohne vorgängige, Einholung der entsprechenden Berechtigung, zu nutzen. Unter derartigen Versuche gehören u.a.

- Passwort-Cracking;
- Abscannen auf Sicherheitslücken;
- Denial-of-Service-Angriffe (Ping Flooding, Abschliessen/Beendigung von Pakets mit unzulässiger Paketgrösse, UDP Flooding, halboffenes TCP Connection Flooding etc.) u.ä.

5. E-Mail Richtlinie

Der Kunde unterlässt den Versuch, E-Mails gegen den erklärten oder mutmasslichen Willen an Dritte zu senden oder Andere durch die Zusendung eines E-Mails zu schikanieren, zu belästigen, zu beleidigen oder sonst zu stören. Dies gilt unabhängig von der Form, Sprache, Häufigkeit oder Grösse der E-Mails. Darunter fällt insbesondere auch der Versand von nicht verlangten grossen E-Mail-Nachrichten, der Versand kommerzieller Werbung, informativer Ankündigungen, religiöser oder politischer Schriften etc. Derartiges Material darf nur an Empfänger gesendet werden, die dieses ausdrücklich verlangt haben. Hierunter fällt auch der Versand von Kettenbriefen.

Für E-Mails, die über den IT-onBase-Dienst gesendet werden oder deren Versand durch den IT-onBase-Dienst verursacht wird, ist Folgendes verboten:

- Verwendung ungültiger oder gefälschter Angaben im E-Mailheader;
- Verwendung ungültiger oder nichtexistierender Domainnamen;
- Anwendung von Methoden, für die anderweitige Falschdarstellung, Verbergung oder Verschleierung von Informationen zur Identifizierung der Herkunft oder des Übermittlungswegs;
- die Verwendung sonstiger Mittel zur Irreführung der Adressierung;
- die Verwendung eines Internet-Domainnamens einer Drittpartei ohne deren Einwilligung, die Weiterleitung Mail über Geräte Dritter ohne deren Genehmigung;
- die Angabe falscher oder irreführender Informationen in der Betreffzeile oder die anderweitige Angabe falscher oder irreführender Inhalte;
- die Verwendung von Marken, Slogans oder Logos der ITOB ohne deren vorherige schriftliche Einwilligung;
- versenden von SPAM-Mails (unverlangte Mails);
- versenden von Newsletter-E-Mails (als Newsletter gelten hundert oder mehr E-Mails mit identischem Inhalt, die innerhalb von vierundzwanzig Stunden versendet werden) über die Shared-Gateway-Infrastruktur ohne schriftliche Genehmigung der ITOB;
- versenden von Newsletter-E-Mails über eigene, virtuelle Systeme ohne vorgängige schriftliche Ankündigung.

Darüber hinaus ist es Ihnen untersagt, den IT-onBase-Dienst für den Versand von E-Mails an:

- gekaufte, gemietete oder ausgeliehene Verteilerlisten zu nutzen;
- Listen, die gemäss den üblichen Branchenpraktiken wahrscheinlich zu einer übermässigen Zahl Spam-Beschwerden oder -Mitteilungen führen würden, zu nutzen.

Schönbühl, 12.11.2018