Anlage 1 – technisch-organisatorische Maßnahmen

Dieses Dokument dient als Ergänzung der Auftragsverarbeitervereinbarung und beschreibt die technischen und organisatorischen Maßnahmen, die von der abaton EDV-Dienstleistungs GmbH als Auftragsverarbeiter zum Schutz der Rechte und Freiheiten von der Auftragsverarbeitung betroffener Personen getroffen wurden bzw. umgesetzt werden.

VERTRAULICHKEIT

Zutrittskontrolle:

Der Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen in den Büroräumlichkeiten erfolgt durch Schlüssel, Alarmanlagen und Videoanlagen. Der Zutritt zu den Rechenzentren der Sub-Auftragsverarbeiter erfolgt durch Schlüssel, Chipkarten, elektrische Türöffner, teilweise Portier, Alarmanlagen und Videoanlagen. Die Rechenzentren sind ISO/IEC 27001 zertifiziert.

Zugangskontrolle:

Der Schutz vor unbefugter Systembenutzung erfolgt durch Kennwörter mit strikten Richtlinien, sowie automatischen Sperrmechanismen (Logout bei Inaktivität). Der Zugang auf die Serverebene (root-Zugriff) ist ebenso nur mit Benutzername und Passwort oder mittels auf dem Server hinterlegter SSH-Keys möglich. Zusätzlich werden Zugriffslisten für IP-Adressen geführt, und damit sichergestellt, dass Zugriffe von nicht berechtigten IP-Adressen technisch gar nicht möglich sind. Die Zugriffe auf die Server werden in entsprechenden Logs auf den Servern erfasst.

Zugriffskontrolle:

Die Berechtigungen werden ausschließlich durch die Administratoren des Auftragnehmers oder der Sub-Auftragsverarbeiter des Auftragnehmers vergeben. Sämtliche Systemzugriffe werden protokolliert. Kennwörter werden in regelmäßigen Abständen geändert.
Bei Ausscheiden von Mitarbeitern aus dem Unternehmen wird der Büroschlüssel retourniert und die Rückgabe dokumentiert. Zusätzlich werden die Accounts gesperrt und etwaige Login-Keys von den Servern entfernt, um zu gewährleisten, dass ausgeschiedene Mitarbeiter keinerlei Datenzugriff mehr haben. Ebenso werden die Zutrittsmöglichkeiten zu den Rechenzentren deaktiviert.

INTEGRITÄT

Weitergabekontrolle:

Zum Schutz gegen unbefugtes Lesen, Kopieren, Verändern oder Entfernen personenbezogener Daten von Betroffenen erfolgt der Zugriff auf die Kundenserver ausschließlich über verschlüsselte Verbindungen.

Eingabekontrolle:

Sämtliche Zugriffe auf die Server werden in den jeweiligen Logs auf den Servern protokolliert. Zur Kontrolle der Dateneingabe oder Datenveränderung in den Content Management Systemen (z.B. TYPO3) verfügen diese im

abaton EDV-Dienstleistungs GmbH
Hans-Resel-Gasse 17, A-8020 Graz
Mariahilfer Straße 1D/13, A-1060 Wien
Tel. +43 5 0240 | Fax DW 70
www.abaton.at | office@abaton.at
FN 202006v, LG für ZRS Graz
UID-Nummer ATU 52569000
Hypobank Steiermark: BIC HYSTAT2G
IBAN AT18 5600 0201 4133 3306

Normalfall über entsprechende Log-Mechanismen. Anhand dieser lässt sich im Anlassfall nachvollziehen, welcher Benutzer zu welchem Zeitpunkt welche Änderungen durchgeführt hat. Auch diese Logs werden abhängig von den Einstellungen im jeweiligen System in regelmäßigen Abständen überschrieben und damit nur für einen definierten Zeitraum aufbewahrt.

VERFÜGBARKEIT UND BELASTBARKEIT

Verfügbarkeitskontrolle:

Unsere Server befinden sich in state of the art-Datenzentren in Wien; diese sind ISO/IEC 27001 zertifiziert und verfügen über redundante Stromkreise inklusive Batteriebackup und redundante Klimaanlagen. Unsere Kundenhardware verfügt über redundante, systemkritische Komponenten und hat seitens des Hardware-Herstellers Mission Critical Support (24 x 7 x 4h vor Ort). Die eigene Infrastruktur wird mit einem Echtzeit-Monitoring überwacht und verständigt automatisch die abaton-Technik (24 Stunden-Support).

Rasche Wiederherstellbarkeit:

Alle unsere Server werden täglich komplett gesichert. Die Sicherung erfolgt in das jeweils andere Rechenzentrum und ist damit off-site. Im Fall eines Desasters, z.B. kompletter Datenverlust eines Servers, wird diese Sicherung für die Wiederherstellung der Daten verwendet. Wenn Kunden durch eigenes Verschulden individuelle Rücksicherungen aus diesem Desaster-Backup benötigen, so wird der damit verbundene Aufwand in Rechnung gestellt.

VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen

Incident-Response-Management:

Die abaton-eigenen Server und Services sind in ein Monitoring-System eingebunden, das im Falle von Problemen und Auffälligkeiten automatisch die abaton-Technik verständigt (24-Stunden-Support). Bei kritischen Vorfällen wird hier unmittelbar mit der Analyse des Problems begonnen. Auch bei Vorfällen die von extern gemeldet werden – z.B. durch den Kunden selbst oder von externen Stellen wie etwa CERT – passiert das Gleiche.

Auftragskontrolle:

Auftragsdatenverarbeitungen die über die normale, laufende Wartung hinaus nötig sind, werden grundsätzlich nur nach entsprechender Weisung des Kunden (Verantwortlichen) durchgeführt. Um zu gewährleisten, dass hier niemand unbefugt Anweisungen erteilen darf, werden die befugten technischen Ansprechpersonen des Kunden in unserer Datenbank bei den jeweiligen Services hinterlegt. Bei einem neuen Datenverarbeitungsauftrag (per E-Mail oder Telefon) wird vorab geprüft, ob der Auftraggeber für das entsprechende System Befugnisse hat, falls nicht wird der Auftrag abgelehnt und der Kunde über den Vorfall informiert.

abaton EDV-Dienstleistungs GmbH
Hans-Resel-Gasse 17, A-8020 Graz
Mariahilfer Straße 1D/13, A-1060 Wien
Tel. +43 5 0240 | Fax DW 70
www.abaton.at | office@abaton.at
FN 202006v, LG für ZRS Graz
UID-Nummer ATU 52569000
Hypobank Steiermark: BIC HYSTAT2G
IBAN AT18 5600 0201 4133 3306