1. Vorwort

1. Der Auftragnehmer gewährleistet die für eine *Auftragsverarbeitung* notwendige Sicherheit der *Verarbeitung* gem. Art. 28 Abs. 3 lit. c, Art. 32 DS-GVO, indem er folgende Verpflichtungen übernimmt:

a) Implementierung der geltenden *TOM* vor Aufnahme der *Auftragsverarbeitung*,

b) Aufrechterhaltung der *TOM* über die Laufzeit der *Auftragsverarbeitung* einschl. etwa nachlaufender Verpflichtungen,

c) Kontrolle der Einhaltung der *TOM* in den gemäß den *TOM* geltenden Zyklen,

d) unverzügliche Nachsteuerung bei Abweichungen vom Sollzustand bei den *TOM*,

e) Kontrolle der Umsetzung der Nachsteuerung sowie

f) Dokumentation der in diesem Rahmen durchgeführten Tätigkeiten einschließlich der dabei gehandhabten Prozesse.

2. Der Auftraggeber informiert sich vor Abschluss der VAV und unter der VAV regelmäßig über die *TOM*. Er trägt die Verantwortung dafür, dass die jeweils geltenden *TOM* für die Risiken der zu *verarbeitenden* Daten ein angemessenes Schutzniveau bieten.

3. Da die *TOM* dem technischen Fortschritt unterliegen, ist es dem Auftragnehmer gestattet, auf eigene Kosten abweichende *TOM* umzusetzen, sofern dabei das Sicherheitsniveau der zuvor festgelegten *TOM* nicht unterschritten wird. Die abweichenden *TOM* werden dokumentiert und auf der in Ziff. I.8. genannten Webseite des Auftragnehmer neu veröffentlicht. Der Auftraggeber erhält eine Mitteilung in Textform über die veränderten *TOM*.

2. Vertraulichkeit

Maßnahmen in den Geschäftsräumen

Die Geschäftsräume der expensebrain GmbH sind als Datenschutzbereich gekennzeichnet und dürfen nur von autorisiertem Personal oder deren Gästen betreten werden. Der Zugang zum Gebäude und den Geschäftsräumen ist durch ein zentrales Schlüssel-System gesichert. Die Vergabe und Rückgabe der Schlüssel erfolgt nur an Mitarbeiter und wird protokolliert. Betriebsfremden ist der Zugang zu den Räumen (bis zu deren Verlassen) nur in ununterbrochener Begleitung eines Mitarbeiters erlaubt. Für Notfälle im Gebäude verfügt die Hausverwaltung über einen Zentralschlüssel auch für unsere Räume.

Berechtigungskonzepte

Benutzerverwaltung:
Der Kreis der Personen mit Zugang zu Systemen und Anwendungen der Datenverarbeitung ist auf das zur Erfüllung der jeweiligen Aufgaben Notwendige beschränkt und in diesem Rahmen konkret festgelegt. Es bestehen konkrete Regelungen für die Vergabe von Berechtigungen gemäß einem den etwaigen Risiken angemessenen Rollen- und Rechtekonzept. Durch die Vergabe eingeschränkter Berechtigungen ist sichergestellt, dass Benutzer nur die im Rahmen ihrer Aufgabenerfüllung erforderlichen Berechtigungen erhalten (Minimalprinzip).

Benutzerkonten:
Benutzer von Systemen und Anwendungen erhalten eine aus Benutzername und Kennwort bestehendes Konto. Für die erstmalige Anmeldung wird ein Standardpasswort vergeben. Nach der ersten Anmeldung ist der Standardpasswort technisch zwingend in ein persönliches Kennwort zu ändern. Bei jeder Anmeldung müssen sich die Benutzer mit Benutzername und Kennwort gegenüber dem System authentifizieren. Bei Austritt eines Beschäftigten oder bei Verlust einer Kennung werden vergebene Benutzerkennungen und sonstige Zugangscodes gesperrt.

Passwort Sicherheit:
Um die Sicherheit von Passwörtern zu gewährleisten, gelten bei der Vergabe systemspezifische Passwortregeln, die von den Benutzern einzuhalten sind.

Unsere internen Passwortvorgaben verlangen

- eine Passwortlänge von mindestens acht Zeichen
- einen ausreichend großen Zeichensatz (mindestens eine natürliche Zahl und ein Sonderzeichen).
- regelmäßige Änderung, mindestens alle 120 Tage. Dabei muss sich das neue Passwort von den letzten fünf verwendeten Passwörtern unterscheiden.
- Passwörter müssen geheim gehalten werden.
- Die Weitergabe von Passwörtern ist untersagt.

Bildschirmsperre:
Nach einer festgelegten Zeit der Abwesenheit vom Arbeitsplatz (nicht länger als 4 Minuten) aktiviert sich automatisch die passwortgeschützte Bildschirmsperre. Bei Verlassen des Arbeitsplatzes ist der Passwortschutz der Bildschirmsperre manuell zu aktivieren

Clean Desk Prinzip:
Bildschirm und Drucker sind stets so aufgestellt, dass sie gegen Einblicke unbefugter Dritter geschützt sind, Bildschirme auch bei Arbeiten außerhalb der Büroräume. Die Beschäftigten sind verpflichtet, Ausdrucke oder Kopien unverzüglich aus Druckern oder Kopiergeräten zu entnehmen. Unterlagen mit personenbezogenen Daten oder vertraulichen Informationen dürfen auf Schreibtischen nicht offen zugänglich hinterlassen, sondern müssen in verschließbaren Schränken abgelegt werden.

WLAN:
ist mit dem Verschlüsselungsalgorithmus wifi protected Access 2 (WPA2) oder besser gesichert. Unverschlüsselte WLAN Netze sollen nicht genutzt werden, auch nicht außerhalb der Büroräume.

3. Integrität

Daten Geheimnis:
alle Beschäftigten sind gemäß den gesetzlichen Vorschriften auf das Datengeheimnis verpflichtet.

Datenwiederherstellung/Backup:
Sämtliche Daten werden redundant gemäss Backup Strategie an getrennten Orten gesichert. Der Zutritt dazu ist mit Schlüsselsystem gesichert. Durch einen Notfallplan können alle Daten im Krisenfall in kürzester Zeit wiederhergestellt werden.

Datenschutzgerechtes Löschen:
Dokumente und Datenträger, die personenbezogene oder sonstige vertrauliche Daten enthalten, werden datenschutzkonform entsorgt. Schriftliche Dokumente werden unter Verwendung eines Schredders der Schutzstufe 4 oder besser (Cross-Cut) vernichtet und entsorgt.

IT Sicherheitsrichtlinien:
Die expensebrain GmbH hat Richtlinien zur IT-Sicherheit erlassen. Alle Beschäftigten sind verpflichtet, die geltenden Sicherheitsrichtlinien zu beachten. Die Sicherheitsrichtlinien werden regelmäßig überprüft und dem Stand der Technik angepasst, falls erforderlich. Soweit technisch möglich, werden Sicherheitseinstellungen über Einstellungen der Hard- und Software systemseitig erzwungen.

4. Innerbetriebliche Organisation

Verfahrensverzeichnis:
Die expensebrain GmbH führt ein laufend aktualisiertes Verfahrensverzeichnis.

Information der Beschäftigten:
alle Beschäftigten sind mit den Themen Datenschutz und Datensicherheit vertraut gemacht und werden in regelmäßigen Abständen darauf hingewiesen und weiter geschult.

Vertrag zur Auftragsdatenverarbeitung:
mit externen Dienstleistern, die personenbezogene Daten im Auftrag verarbeiten, bestehen grundsätzlich schriftliche Verträge zur Auftragsdatenverarbeitung.

Notfallkonzept:
Die expensebrain GmbH hat ein Notfallkonzept für die Daten der Kunden implementiert. Auf diese Weise ist sie optimal auf die Bewältigung eines Notfalls oder eine Krise vorbereitet; die Wahrscheinlichkeit eines Schadenseintritts ist minimiert.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen:

Sämtliche technischen und organisatorischen Maßnahmen werden regelmäßig überprüft und entsprechend sich etwa entwickelnder Risiken und dem sich ändernden Stand der Technik (unter Berücksichtigung auch der Implementierungskosten) angepasst.

5. Dienstleister

Website

Wir erheben und verarbeiten selbst keine kundenbezogenen Daten über die Website. Für die Nutzung von Diensten innerhalb der Website gelten die Datenschutzerklärungen der Anbieter unter https://www.expensebrain.de/datenschutz

Maßnahmen im Rechenzentrum des Hosting Providers

Unsere Website wird gehostet bei Hetzner mit Datenzentren in Deutschland und Finnland.

Die ToM unseres Hosting Partners Hetzner finden Sie unter https://www.hetzner.com/AV/TOM.pdf.