Technischen und organisatorische Maßnahmen gem. Artt. 28 Abs. 3 lit. c und 32 DS-GVO

1. Vertraulichkeit (confidentiality)

1.1. Der körperliche Zutritt von Personen in Räumlichkeiten von Pink & Adel ist nur nach vorheriger Legitimation möglich. Zum Einsatz kommen herkömmliche Sicherheitsschlösser, zu denen die Schlüssel ausschließlich an berechtigte Mitarbeiter ausgegeben werden.

1.2. Der Kreis der Zutrittsberechtigten ist festgelegt.

1.3. Besucher müssen an der Eingangstür klingeln und werden durch Mitarbeiter von Pink & Adel eingelassen.

1.4. Besucher werden durchgehend begleitet.

1.5. Die Mitarbeiter sind schriftlich auf die Vertraulichkeit, bzw. das Datengeheimnis verpflichtet.

1.6. Der Zugang zu Workstations und Notebooks ist über individuelle Benutzerkonten geschützt.

1.7. Es wird unterschieden zwischen „normalen“ Benutzern und Administratoren.

1.8. Kein Einsatz von Sammelusern.

1.9. Die Anmeldung an Servern ist über gesonderte Administrator-Konten geschützt, die ausschließlich durch berechtigte Administratoren genutzt werden.

1.10. Die Vergabe jeglicher Benutzerkonten wird durch die Geschäftsleitung freigegeben.

1.11. Zugangsberechtigungen zu Rechnern werden personengebunden vergeben.

1.12. Zugangsberechtigungen werden auch für Netzwerklaufwerke personengebunden vergeben.

1.13. Der Kreis der jeweils befugten Personen ist auf das betriebsnotwendige Maß eingeschränkt.

1.14. Wo technisch möglich, wird eine 2-Faktor-Authentifizierung genutzt.

1.15. Zugriffsberechtigungen werden in den Anwendungen rollenbasiert vergeben. Es wird nach dem Prinzip „need-to-know“ und „need-to-do“ verfahren.

1.16. Die Verwaltung der Rollen erfolgt in den Anwendungen.

1.17. Jeder Zugangsberechtigte kann nur auf Daten zugreifen, die er zur Ausübung der ihm übertragenen Aufgaben und Funktionen benötigt.

1.18. Mandantentrennung in den Anwendungen von Pink & Adel.

1.19. Getrennte Datenbanken für unterschiedliche Anwendungen.

1.20. Es findet keine lokale Speicherung von personenbezogenen Daten statt. Sämtliche Daten werden zentral auf Servern gespeichert.

1.21. Die Datenübertragung mit und zwischen den Systemen von Pink & Adel erfolgt verschlüsselt.

1.22. Die Festplatten mobiler Rechner sind grundsätzlich verschlüsselt.

1.23. E-Mails können Ende-zu-Ende verschlüsselt (PGP) versandt und empfangen werden. Schlüssel werden pro E-Mailadresse erstellt.

1.24. Im Rahmen von Datenverarbeitungen im Auftrag verarbeitet Pink & Adel die überlassenen personenbezogenen Daten ausschließlich aufgrund und anhand von vertraglichen vereinbarten Weisungen des Auftraggebers.

1.25. Pink & Adel unterstützt die Auftraggeber bei der Ausübung ihrer Kontrollpflichten.

1.26. Pink & Adel führt in unregelmäßigen Abständen stichprobenartige interne Auftragskontrollen durch.

1.27. Mit Dienstleistern und Subunternehmern werden Verträge zur Auftrags(daten)verarbeitung geschlossen, welche Regelungen enthalten, mit denen die in dieser Bestätigung enthaltenen Maßnahmen auch den Dienstleistern auferlegt werden.

2. Integrität (integrity)

2.1. Zugriffsberechtigungen werden in den Anwendungen rollenbasiert vergeben. Es wird nach dem Prinzip „need-to-know“ und „need-to-do“ verfahren.

2.2. Die Mitarbeiter sind schriftlich auf die Vertraulichkeit, bzw. das Datengeheimnis verpflichtet.

2.3. Pink & Adel sichert seine Systeme über Virensoftware und Firewall ab.

2.4. Personenbezogene Daten werden bei Wegfall des Verarbeitungsgrunds gelöscht. Gesetzliche sowie vertragliche Aufbewahrungspflichten werden dabei beachtet.

2.5. Sachbearbeiter und Zeitpunkt von Verarbeitungen werden automatisch protokolliert.

2.6. Die Protokolle sind vor unbefugtem Zugriff geschützt.

2.7. Im Rahmen von Datenverarbeitungen im Auftrag verarbeitet Pink & Adel die überlassenen personenbezogenen Daten ausschließlich aufgrund und anhand von vertraglichen vereinbarten Weisungen des Auftraggebers.

2.8. Jeder Zugangsberechtigte kann nur auf Daten zugreifen, die er zur Ausübung der ihm übertragenen Funktionen benötigt.

2.9. Mandantentrennung in den Anwendungen von Pink & Adel.

2.10. Getrennte Datenbanken für unterschiedliche Anwendungen.

2.11. Die Datenübertragung mit und zwischen den Systemen von Pink & Adel erfolgt verschlüsselt.

2.12. E-Mails können Ende-zu-Ende verschlüsselt (PGP) versandt und empfangen werden. Schlüssel werden pro E-Mailadresse erstellt.

2.13. Im Rahmen von Datenverarbeitungen im Auftrag verarbeitet Pink & Adel die überlassenen personenbezogenen Daten ausschließlich aufgrund und anhand von vertraglichen vereinbarten Weisungen des Auftraggebers.

2.14. Pink & Adel führt in unregelmäßigen Abständen stichprobenartige interne Auftragskontrollen durch.

3. Verfügbarkeit (availability)

3.1. Die Anmeldung an Servern ist über gesonderte Administrator-Konten geschützt, die ausschließlich durch berechtigte Administratoren genutzt werden.

3.2. Die Vergabe jeglicher Benutzerkonten wird durch die Geschäftsleitung freigegeben.

3.3. Zugangsberechtigungen zur Rechnern werden personengebunden vergeben.

3.4. Zugangsberechtigungen werden auch für Netzwerklaufwerke personengebunden vergeben.

3.5. Der Kreis der jeweils befugten Personen ist auf das betriebsnotwendige Maß eingeschränkt.

3.6. Zugriffsberechtigungen werden in den Anwendungen rollenbasiert vergeben. Es wird nach dem Prinzip „need-to-know“ und „need-to-do“ verfahren.

3.7. Die Verwaltung der Rollen erfolgt in den Anwendungen.

3.8. Jeder Zugangsberechtigte kann nur auf Daten zugreifen, die er zur Ausübung der ihm übertragenen Funktionen benötigt.

3.9. Sachbearbeiter und Zeitpunkt von Verarbeitungen werden automatisch protokolliert, die Protokolle sind vor unbefugtem Zugriff geschützt.

3.10. Pink & Adel sichert seine Systeme über Virensoftware und Firewall ab.

3.11. Es findet keine lokale Datenhaltung auf Workstations statt.

3.12. Es werden täglich, sowie vor Deployment neuer Funktionalitäten Backups der Datenbanken und Server erstellt.

3.13. Die Backups werden außerhalb der Räume von Pink & Adel gelagert.

3.14. Pink & Adel führt in unregelmäßigen Abständen stichprobenartige interne Auftragskontrollen durch.

3.15. Mit Dienstleistern und Subunternehmern werden Verträge zur Auftrags(daten)verarbeitung geschlossen, welche Regelungen enthalten, mit denen die in dieser Bestätigung enthaltenen Maßnahmen auch den Dienstleistern auferlegt werden.

4. Belastbarkeit (resilience)

4.1. Pink & Adel sichert seine Systeme über Virensoftware und Firewall ab.

4.2. Es findet keine lokale Datenhaltung auf Workstations statt.

4.3. Es existieren verteilte Systeme und Rechenzentren an unterschiedlichen Standorten.

4.4. Es werden täglich, sowie vor Deployment neuer Funktionalitäten Backups der Datenbanken und Server erstellt.