Anlage 1:

Technische und organisatorische Maßnahmen i.S.d. Art. 32 DSGVO

1. Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

- ☒ Einsatz kryptographischer Verfahren wie beispielweise getunnelte Datenfernverbindungen (VPN) mit 256 Bit AES Verschlüsselung
- ☒ Zugriffsprotokolle mit SSL-Verschlüsselung
- ☒ Komprimierung der Daten bei Nutzung des Fernwartungszugangs
- ☒ Verschlüsselung von Datensätzen sowie unserer Backup Medien
- ☒ Verschlüsselung (Transportebene) des Mail Versands

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- ☒ Alarmanlage
- ☒ Bewegungsmelder
- ☒ Schlüsselregelung (Schlüsselausgabe etc.)
- ☒ Protokollierung der Besucher
- ☒ Sorgfältige Auswahl von Wachpersonal
- ☒ Absicherung von Gebäudeschächten
- ☒ Chipkarten-/Transponder-Schließsystem
- ☒ Manuelles Schließsystem
- ☒ Videoüberwachung der Zugänge
- ☒ Sicherheitsschlösser
- ☒ Personenkontrolle beim Empfang
- ☒ Sorgfältige Auswahl von Reinigungspersonal

2.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Bezogen auf interne Systeme der FLOWFACT.

- ☒ Zuordnung von Benutzerrechten
- ☒ Passwortvergabe
- ☒ Authentifikation mit Benutzername / Passwort
- ☒ Einsatz einer Hardware-Firewall
- ☒ Einsatz einer Software-Firewall
- ☒ Zuordnung von Benutzerprofilen zu IT-Systemen
- ☒ Einsatz von VPN-Technologie
- ☒ Sicherheitsschlösser

- ☒ Schlüsselregelung (Schlüsselausgabe etc.)
- ☒ Personenkontrolle beim Empfang
- ☒ Protokollierung der Besucher
- ☒ Sorgfältige Auswahl von Reinigungspersonal
- ☒ Sorgfältige Auswahl von Wachpersonal
- ☒ Erstellen von Benutzerprofilen
- ☒ Einsatz von Intrusion-Detection-Systemen
- ☒ Verschlüsselung von mobilen Datenträgern
- ☒ Einsatz von Anti-Viren-Software

2.3 Zugriffs- und Datenträgerkontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (Zugriffskontrolle) und Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle)

- ☒ Erstellen eines Berechtigungskonzepts
- ☒ Verwaltung der Rechte durch Systemadministrator
- ☒ Anzahl der Administratoren auf das „Notwendigste“ reduziert
- ☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- ☒ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ☒ Sichere Aufbewahrung von Datenträgern
- ☒ physische Löschung von Datenträgern vor Wiederverwendung
- ☒ ordnungsgemäße Vernichtung von Datenträgern (etwa DIN 66399)
- ☒ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- ☒ Protokollierung der Vernichtung
- ☒ Verschlüsselung von Datenträgern

2.4 Trennbarkeit

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit)

- ☒ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☒ Festlegung von Datenbankrechten
- ☒ Erstellung eines Berechtigungskonzepts
- ☒ Logische Mandantentrennung (softwareseitig)
- ☒ Versehen der Datensätze mit Zweckattributen/Datenfeldern
- ☒ Trennung von Produktiv- und Testsystem (Netzwerksegmentierung durch Account- und Netzwerktrennung)

3. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Übertragungs- und Transportkontrolle

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle) und dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle)

- ☒ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☒ E-Mail-Verschlüsselung
- ☒ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen
- ☒ Beim physischen Transport: sichere Transportbehälter/-verpackungen

3.2 Eingabe- und Speicherkontrolle

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle) und Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle)

- ☒ Protokollierung der Eingabe, Änderung und Löschung von Daten
- ☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- ☒ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.

4. Verfügbar- und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

4.1 Verfügbarkeit

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)

- ☒ Unterbrechungsfreie Stromversorgung (USV)
- ☒ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☒ Feuer- und Rauchmeldeanlagen
- ☒ Testen von Datenwiederherstellung
- ☒ Klimaanlage in Serverräumen
- ☒ Schutzsteckdosenleisten in Serverräumen
- ☒ Feuerlöschgeräte in Serverräumen
- ☒ Erstellen eines Backup- & Recoverykonzepts

☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

☒ Erstellen eines Notfallplans

4.2 Belastbarkeit der Systeme

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität)

☒ Regelmäßige Überprüfung der Betriebsbereitschaft aller Funktionen der Systeme

☒ Regelmäßige Wartung der Systeme

☒ Automatisierte Meldung von Fehlfunktionen

☒ Routinemaßnahmen zur Absicherung der Systeme bei Fehlermeldungen

☒ Virenschutz

☒ Firewalls

☒ Durchführung einer Risiko- und Schwachpunktanalyse

☒ Ständige Aktualisierung der genutzten Software

☒ Funktionale Trennung zwischen IT-Abteilung und anderen Abteilungen

5. Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (Art. 32 Abs. 1 lit. c DSGVO)

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit)

☒ Erstellung von Sicherheitskopien in regelmäßigen Abständen

☒ Speicherung der Sicherheitskopien an einem sicheren Ort außerhalb der IT-Abteilung

☒ Prüfung der Wiederherstellungsfähigkeit der Sicherheitskopien in regelmäßigen Abständen

☒ Datenwiederherstellungsprozeduren

☒ Datenspiegelungen

☒ Festgelegte Aufbewahrungszeit der Sicherungskopien

☒ Gewährleistung der Aktualität der Sicherungskopien, Rhythmus der Sicherung und des Mediums:

- Täglich D2D (auf Backupserver)
- Täglich auf Band

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d, 25 Abs. 1 DSGVO)

6.1 Auftragskontrolle

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle)

- ☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- ☒ Vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- ☒ Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. Art. 28 Abs. 3 DSGVO
- ☒ Schriftliche Verpflichtung der Mitarbeiter des Auftragnehmers zur Vertraulichkeit
- ☒ Auftragnehmer hat Datenschutzbeauftragten bestellt
- ☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☒ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- ☒ Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

6.2 Datenschutz-Management

- ☒ Interne Datenverarbeitungsrichtlinien, -verfahren, Leitlinien, Arbeitsanweisungen, Verfahrensbeschreibungen und -regelungen für die Programmierung, Überprüfung und Veröffentlichung von Daten
- ☒ Vorhandenes Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der ergriffenen technischen und organisatorischen Maßnahmen
- ☒ Überprüfung der Systeme und Programme nach Industriestandards
- ☒ Regelmäßige Schulungen der Mitarbeiter
- ☒ Vier-Augen-Prinzip
- ☒ Vorliegen eines Datensicherheitskonzepts
- ☒ Bestehen eines Verzeichnisses von Verarbeitungstätigkeiten
- ☒ Regelmäßige Prüfung der Einhaltung der technischen und organisatorischen Maßnahmen
- ☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (u.a. im Hinblick auf die Meldepflicht gegenüber Aufsichtsbehörde / Betroffenen)
- ☒ Einbindung von DSB in Sicherheitsvorfälle und Datenpannen

6.3 Datenschutzfreundliche Voreinstellungen

- ☒ Berücksichtigung des Grundsatzes der Datenminimierung
- ☒ Aktualisierung der Datenverarbeitung nach dem Stand der Technik