Anlage 1 – Technische und organisatorische Maßnahmen (TOM)

der Post-Consulting GmbH

gemäß Art. 28 Abs. 3 lit. c, Art. 32 und Art. 25 DSGVO

Vorbemerkung

Die Post-Consulting GmbH trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen angemessene technische und organisatorische Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus.

Die Maßnahmen berücksichtigen insbesondere, dass im Rahmen der vereinbarten Dienstleistungen personenbezogene Daten sowie besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO, insbesondere Gesundheitsdaten, und Informationen verarbeitet werden können, die einem Berufsgeheimnis gemäß § 203 StGB unterliegen.

Die nachfolgenden Maßnahmen werden regelmäßig sowie anlassbezogen auf ihre Wirksamkeit überprüft und erforderlichenfalls unter Berücksichtigung veränderter Risiken und des Stands der Technik angepasst.

1. Vertraulichkeit

1.1 Physische Zutrittskontrolle

Ziel ist die Verhinderung des unbefugten physischen Zutritts zu Gebäuden, Räumen und Einrichtungen, in denen personenbezogene Daten verarbeitet werden.

Umgesetzte Maßnahmen:

1. Elektronische Zutrittskontrolle an den Standorten sowie zusätzliche Zutrittsbeschränkungen für besonders schutzbedürftige Bereiche, insbesondere Server- und Produktionsbereiche.
2. Zutritt betriebsfremder Personen und externer Dienstleister nur im erforderlichen Umfang und nach entsprechender Legitimation bzw. Authentisierung sowie erforderlichenfalls in Begleitung berechtigter Mitarbeiter.
3. Einsatz von Einbruchmeldeanlagen sowie geeigneter technischer und organisatorischer Maßnahmen zur Überwachung und Sicherung der Zutritte an Produktions- und IT-Standorten.
4. Vergabe von Zutrittsberechtigungen ausschließlich an hierzu berechtigte Personen nach festgelegten Zuständigkeiten und einer entsprechenden Berechtigungsmatrix.
5. Überprüfung und erforderlichenfalls Anpassung bzw. Entziehung von Zutrittsberechtigungen bei Änderungen der Tätigkeit oder beim Ausscheiden von Mitarbeitern.

1.2 Elektronische Zugangskontrolle

Ziel ist die Verhinderung einer unbefugten Nutzung der zur Verarbeitung personenbezogener Daten eingesetzten IT-Systeme.

Umgesetzte Maßnahmen:

1. Berechtigungskonzept für den Zugang zu den eingesetzten IT-Systemen.
2. Verwendung individuell zugeordneter bzw. personalisierter Benutzerkennungen.
3. Authentisierung berechtigter Nutzer vor Zugang zu den jeweiligen Systemen.
4. Betrieb der Produktions- und Verarbeitungssysteme innerhalb einer gesicherten Netzwerkumgebung.
5. Schutz der Netzwerkumgebung durch Firewall-Systeme sowie geeignete Netzwerksegmentierung bzw. DMZ-Strukturen.
6. Dateneinlieferung und Datenabruf ausschließlich durch autorisierte Nutzer bzw. Systeme.
7. Verschlüsselte Datenübertragung über gesicherte Übertragungswege, insbesondere SFTP sowie TLS/HTTPS beim Webportal.
8. Vergabe von Zugangsberechtigungen nach dem Erforderlichkeitsprinzip.

1.3 Interne Zugriffskontrolle

Ziel ist sicherzustellen, dass berechtigte Nutzer ausschließlich auf diejenigen personenbezogenen Daten zugreifen können, die sie zur Erfüllung ihrer jeweiligen Aufgaben benötigen.

Umgesetzte Maßnahmen:

1. Rollen- und Berechtigungskonzept für IT- und Produktionssysteme.
2. Vergabe von Zugriffsrechten nach dem Erforderlichkeits- und Need-to-know-Prinzip.
3. Beschränkung des Zugriffs auf personenbezogene Daten auf hierzu berechtigte Mitarbeiter.
4. Protokollierung sicherheits- und verarbeitungsrelevanter Zugriffe und Vorgänge, soweit technisch vorgesehen und erforderlich.
5. Überprüfung und erforderlichenfalls Anpassung bestehender Benutzer- und Zugriffsberechtigungen.

6. Entziehung bzw. Sperrung von Berechtigungen bei Ausscheiden eines Mitarbeiters oder entsprechender Änderung seines Aufgabenbereichs.

1.4 Verpflichtung auf Vertraulichkeit und Geheimhaltung

Umgesetzte Maßnahmen:

1. Verpflichtung der mit personenbezogenen Daten befassten Mitarbeiter auf Vertraulichkeit.
2. Abschluss gesonderter Geheimhaltungsvereinbarungen mit den Mitarbeitern.
3. Unterrichtung und Verpflichtung der betreffenden Mitarbeiter hinsichtlich der Wahrung von Berufsgeheimnissen gemäß § 203 StGB, soweit solche Informationen im Rahmen ihrer Tätigkeit zugänglich werden können.
4. Beachtung der gesetzlichen Verpflichtungen zur Wahrung des Postgeheimnisses.
5. Beschränkung der Kenntnisnahme von Dokument- und Inhaltsdaten auf das für die jeweilige Tätigkeit erforderliche Maß.
6. Regelmäßige Schulung und Sensibilisierung der Mitarbeiter zu Datenschutz, Informationssicherheit und Vertraulichkeit.

2. Trennung, Datenminimierung und Pseudonymisierung

2.1 Trennung nach Auftraggeber und Auftrag

Umgesetzte Maßnahmen:

1. Logische bzw. serielle Trennung der Verarbeitung nach Auftraggeber und Auftrag.
2. Eindeutige Zuordnung und Kennzeichnung der jeweiligen Verarbeitungsaufträge.
3. Vermeidung einer Vermischung von Daten unterschiedlicher Auftraggeber innerhalb des Produktionsprozesses.
4. Verarbeitung ausschließlich der für den jeweiligen Auftrag erforderlichen Daten.

2.2 Datenminimierung und Pseudonymisierung

Eine vollständige Pseudonymisierung der für die Briefproduktion und den postalischen Versand erforderlichen Empfängerdaten ist aufgrund des Verarbeitungszwecks nicht möglich, da insbesondere Name und Anschrift des Empfängers für die Herstellung und Zustellung der Sendung erforderlich sind.

Soweit für einzelne Verarbeitungsschritte keine unmittelbare Personenbeziehbarkeit erforderlich ist, wird die Verarbeitung auf die jeweils erforderlichen Daten beschränkt.

Personenbezogene Daten werden nur in dem für den jeweiligen Verarbeitungszweck erforderlichen Umfang und Zeitraum verarbeitet.

3. Integrität und Übertragungskontrolle

Ziel ist der Schutz personenbezogener Daten gegen unbefugte Kenntnisnahme, Veränderung, Verlust oder sonstige unzulässige Verarbeitung während der Übermittlung und Verarbeitung.

Umgesetzte Maßnahmen:

1. Verschlüsselte elektronische Übertragung personenbezogener Daten über hierfür vorgesehene gesicherte Übertragungswege.
2. Gesicherter Datenaustausch insbesondere über SFTP sowie TLS/HTTPS beim Webportal.
3. Beschränkung der Datenübermittlung und des Datenabrufs auf autorisierte Nutzer und Systeme.
4. Gesicherte interne Übertragung innerhalb der vorgesehenen Netzwerk- und Systemumgebung.
5. Protokollierung sicherheits- und verarbeitungsrelevanter Übertragungsvorgänge, soweit technisch vorgesehen und erforderlich.
6. Zugriff auf Verarbeitungssysteme ausschließlich durch hierzu berechtigte Nutzer.
7. Eindeutige Zuordnung der jeweiligen Benutzer- und Verarbeitungsberechtigungen.
8. Schutz der Verarbeitungssysteme vor unbefugten Veränderungen.
9. Übergabe fertiggestellter Dokumente an den postalischen Beförderungsprozess ausschließlich als ordnungsgemäß verschlossene Sendungen.
10. Schutz der fertiggestellten Sendungen bis zur Übergabe an den jeweiligen Post-, Beförderungs- oder Transportdienstleister.

4. Löschung und Speicherbegrenzung

Ziel ist die Beschränkung der Speicherung personenbezogener Daten auf den zur Durchführung des jeweiligen Auftrags erforderlichen Zeitraum.

Umgesetzte Maßnahmen:

1. Festgelegte Löschprozesse und automatisierte Löschroutinen für nicht mehr erforderliche Produktions- und Verarbeitungsdaten.

2. Die zur Produktion vorgehaltenen PDF-Dokumente und Empfängerdaten, insbesondere Name und Anschrift des Empfängers, werden nach Abschluss des jeweiligen Verarbeitungs- und Versandprozesses automatisiert aus dem hierfür vorgesehenen System gelöscht.
3. Die Löschung erfolgt werktags grundsätzlich innerhalb von 24 Stunden nach Abschluss der Verarbeitung. Bei außerhalb der werktäglichen Verarbeitungszeiten sowie an Wochenenden oder Feiertagen eingestellten Aufträgen erfolgt die Verarbeitung und anschließende Löschung im Rahmen des nächstmöglichen regulären Verarbeitungslaufs.
4. Über SFTP zur Verarbeitung bereitgestellte Dateien werden nach erfolgreicher Übernahme aus dem hierfür vorgesehenen Übertragungsbereich gelöscht.
5. Im Kundenportal kann nach Abschluss des Auftrags ausschließlich die Bezeichnung bzw. der Dateiname des jeweiligen Versandauftrags als Bestandteil der Auftragshistorie verbleiben. Der Inhalt der ursprünglich übermittelten PDF-Datei wird hierdurch nicht gespeichert.
6. Die Speicherung personenbezogener Daten wird auf das für den jeweiligen Zweck erforderliche Maß beschränkt.
7. Nicht mehr erforderliche Datenträger und physische Unterlagen werden entsprechend ihrem Schutzbedarf sicher gelöscht bzw. datenschutzgerecht vernichtet.

5. Verfügbarkeit und Belastbarkeit
Ziel ist der Schutz personenbezogener Daten und der für ihre Verarbeitung eingesetzten Systeme gegen unbeabsichtigte oder unrechtmäßige Zerstörung, Verlust und Ausfall.

Umgesetzte Maßnahmen:
1. Einsatz geeigneter Firewall-Systeme.
2. Einsatz von Schutzmaßnahmen gegen Schadsoftware.
3. Regelmäßige Datensicherungen nach festgelegten Sicherungsprozessen.
4. Sichere bzw. räumlich getrennte Aufbewahrung relevanter Datensicherungen.
5. Notfallhandbuch und festgelegte interne Melde- und Eskalationswege.
6. Notfallübungen im Rahmen der bestehenden Notfall- und Sicherheitsorganisation.
7. Ausreichend dimensionierte IT-Infrastruktur.
8. Einsatz virtualisierter IT-Infrastruktur, soweit dies für die jeweiligen Systeme vorgesehen ist.
9. Maßnahmen zur Sicherstellung der Verfügbarkeit und Belastbarkeit der für die Verarbeitung wesentlichen Systeme.

Datensicherungen unterliegen festgelegten Sicherungs-, Aufbewahrungs- und Überschreibungszyklen. Bei Wiederherstellungen wird berücksichtigt, dass bereits gelöschte bzw. nicht mehr erforderliche personenbezogene Daten nicht erneut einer regulären produktiven Verarbeitung zugeführt werden.

6. Wiederherstellbarkeit
Ziel ist die Fähigkeit, die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen nach einem physischen oder technischen Zwischenfall innerhalb eines angemessenen Zeitraums wiederherzustellen.

Umgesetzte Maßnahmen:
1. Virtualisierte IT-Infrastruktur, soweit für die jeweiligen Systeme eingesetzt.
2. Regelmäßige Datensicherungen nach festgelegten Sicherungsprozessen.
3. Verfahren zur Wiederherstellung betriebsnotwendiger Systeme und Daten nach technischen oder physischen Zwischenfällen.
4. Notfall- und Wiederanlaufplanung für wesentliche Verarbeitungssysteme.
5. Überprüfung der Funktionsfähigkeit der Datensicherungs- und Wiederherstellungsverfahren.
6. Ausreichende Dimensionierung der für die Leistungserbringung erforderlichen IT-Infrastruktur.

7. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Umgesetzte Maßnahmen:
1. Beschränkung der Verarbeitung und Speicherung personenbezogener Daten auf das für den jeweiligen Verarbeitungszweck erforderliche Maß.
2. Automatisierte Löschroutinen für nicht mehr erforderliche Produktions- und Verarbeitungsdaten.
3. Beschränkung von Benutzer- und Systemberechtigungen nach dem Erforderlichkeitsprinzip.
4. Trennung der Verarbeitung nach Auftraggeber und Auftrag.
5. Berücksichtigung von Datenschutz- und Informationssicherheitsanforderungen bei der Gestaltung und Änderung der eingesetzten Systeme und Prozesse.
6. Überprüfung bestehender Prozesse auf Möglichkeiten zur weiteren Datenminimierung.

8. Auftrags- und Verarbeitungskontrolle
Ziel ist sicherzustellen, dass personenbezogene Daten im Rahmen der Auftragsverarbeitung ausschließlich entsprechend den dokumentierten Weisungen des Auftraggebers und den vertraglich vereinbarten Leistungen verarbeitet werden.

Umgesetzte Maßnahmen:

1. Verarbeitung personenbezogener Daten ausschließlich im Rahmen der vertraglich vereinbarten Leistungen und dokumentierten Weisungen des Auftraggebers.
2. Abschluss von Vereinbarungen zur Auftragsverarbeitung gemäß Art. 28 DSGVO.
3. Vertragliche Festlegung von Gegenstand und Dauer sowie Art und Zweck der Verarbeitung, Arten personenbezogener Daten und Kategorien betroffener Personen.
4. Verpflichtung der mit der Verarbeitung betrauten Mitarbeiter auf Vertraulichkeit und Geheimhaltung.
5. Berücksichtigung der besonderen Anforderungen des § 203 StGB, soweit Berufsgeheimnisse verarbeitet werden.
6. Geregelte Auswahl und Überprüfung eingesetzter weiterer Auftragsverarbeiter.
7. Abschluss der erforderlichen Vereinbarungen gemäß Art. 28 DSGVO mit weiteren Auftragsverarbeitern.
8. Festgelegte Lösch- und Verarbeitungsprozesse nach Abschluss des jeweiligen Auftrags.
9. Regelung und Kontrolle der Zugriffs- und Verarbeitungsberechtigungen.

9. Datenschutz-, Informationssicherheits- und Managementsystem

Die Post-Consulting GmbH unterhält ein integriertes Managementsystem und ist nach ISO 9001 (Qualitätsmanagement), ISO 14001 (Umweltmanagement) sowie ISO/IEC 27001 (Informationssicherheitsmanagement) zertifiziert.

Das Informationssicherheitsmanagementsystem nach ISO/IEC 27001 bildet einen wesentlichen Bestandteil der systematischen Steuerung und kontinuierlichen Verbesserung der Informationssicherheit.

Umgesetzte Maßnahmen:

1. Betrieb eines zertifizierten Informationssicherheitsmanagementsystems nach ISO/IEC 27001.
2. Betrieb eines zertifizierten Qualitätsmanagementsystems nach ISO 9001.
3. Betrieb eines zertifizierten Umweltmanagementsystems nach ISO 14001.
4. Festgelegte Verantwortlichkeiten und Prozesse für Datenschutz und Informationssicherheit.
5. Regelmäßige Schulung und Sensibilisierung der Mitarbeiter zu Datenschutz, Informationssicherheit, Vertraulichkeit und einschlägigen Geheimhaltungspflichten.
6. Durchführung regelmäßiger interner und externer Audits im Rahmen der bestehenden Managementsysteme.
7. Dokumentation und regelmäßige Überprüfung der für Datenschutz und Informationssicherheit relevanten Prozesse und Maßnahmen.
8. Regelmäßige sowie anlassbezogene Bewertung der technischen und organisatorischen Maßnahmen.
9. Kontinuierlicher Verbesserungsprozess zur Weiterentwicklung der organisatorischen und technischen Sicherheitsmaßnahmen.

10. Reaktions- und Vorfallmanagement

Ziel ist die frühzeitige Erkennung, Bewertung, Behandlung und Dokumentation von Datenschutz- und Informationssicherheitsvorfällen.

Umgesetzte Maßnahmen:

1. Festgelegte interne Ansprechpartner bzw. Meldestellen für Datenschutz- und Informationssicherheitsvorfälle.
2. Festgelegte interne Melde- und Eskalationswege.
3. Dokumentierter Prozess zur Erkennung, Bewertung, Behandlung und Dokumentation von Datenschutz- und Informationssicherheitsvorfällen.
4. Unverzügliche interne Eskalation möglicher Verletzungen des Schutzes personenbezogener Daten.
5. Verfahren zur unverzüglichen Information des jeweiligen Auftraggebers bei Verletzungen des Schutzes der in seinem Auftrag verarbeiteten personenbezogenen Daten entsprechend den gesetzlichen und vertraglichen Verpflichtungen.
6. Analyse eingetretener Sicherheitsvorfälle und erforderlichenfalls Umsetzung geeigneter Abstell-, Korrektur- und Verbesserungsmaßnahmen.

11. Hosting und weitere Auftragsverarbeiter

Für die Bereitstellung der technischen Hosting- und Serverinfrastruktur für den gesicherten SFTP-Datenaustausch und das Webportal wird insbesondere die IONOS SE als weiterer Auftragsverarbeiter eingesetzt.

Mit eingesetzten weiteren Auftragsverarbeitern werden die nach Art. 28 DSGVO erforderlichen vertraglichen Vereinbarungen geschlossen.
Die Auswahl und Einbindung weiterer Auftragsverarbeiter erfolgt nach festgelegten datenschutzrechtlichen und informationssicherheitsbezogenen Anforderungen. Die von den weiteren Auftragsverarbeitern für die jeweilige Leistung eingesetzten technischen und organisatorischen Maßnahmen werden im Rahmen der gesetzlichen und vertraglichen Anforderungen berücksichtigt.

Soweit bei extern bereitgestellten Diensten zusätzliche Sicherheitsfunktionen, insbesondere erweiterte Authentisierungs-, Verschlüsselungs- oder Datensicherungsfunktionen, verfügbar sind, werden diese unter Berücksichtigung des jeweiligen Schutzbedarfs, des konkreten Dienstes und der bestehenden technischen Konfiguration bewertet.

12. Regelmäßige Überprüfung und Weiterentwicklung

Die Post-Consulting GmbH überprüft die Angemessenheit und Wirksamkeit der technischen und organisatorischen Maßnahmen regelmäßig sowie anlassbezogen.

Dabei werden insbesondere berücksichtigt:

- Änderungen der eingesetzten Systeme, Anwendungen und Verarbeitungsverfahren,
- Veränderungen der Risikolage,
- Art und Schutzbedarf der verarbeiteten Daten, insbesondere Gesundheitsdaten und sonstige besondere Kategorien personenbezogener Daten,
- Sicherheits- und Datenschutzvorfälle,
- Erkenntnisse aus internen und externen Audits,
- Erkenntnisse aus dem Informationssicherheitsmanagementsystem nach ISO/IEC 27001 sowie
- die Weiterentwicklung des Stands der Technik.

Festgestellte Verbesserungsmöglichkeiten werden bewertet und erforderliche technische oder organisatorische Maßnahmen im Rahmen des bestehenden Management- und Informationssicherheitssystems umgesetzt.

Stand: [08/2026] Version 2
Post-Consulting GmbH