# Datenschutz und Datensicherheit der FP IAB - internet access GmbH

Als datenverarbeitendes Systemhaus und Postdienstleister (zertifizierter Software-, Druck- und Versanddienstleister der Deutschen Post AG) und insbesondere als Dienstleister für den öffentlichen Sektor, d.h. für den Staat, werden an uns höchste Anforderungen zum Thema Datenschutz und Datensicherheit gestellt.

Bei unserer Kundenbetreuung nehmen daher der Datenschutz und die Datensicherheit höchste Priorität ein, sie sind zur Erfüllung unserer Dienstleistungen eine Grundvoraussetzung.

So sind wir den gesetzlichen Datenschutzbestimmungen uneingeschränkt verpflichtet nach dem Bundesdatenschutzgesetz (BDSG), dem Fernmeldegeheimnis des Telekommunikationsgesetzes (TKG), dem Briefgeheimnis der Deutschen Post AG sowie als Dienstleister für den öffentlichen Dienst der jeweiligen Stadt, Gemeinde oder Kommune, bspw. dem Wahlamt oder der Oberfinanzdirektion.

Unsere Erfahrungen im Umgang mit „sensiblen“ Daten basieren dabei auf enger Zusammenarbeit mit vielen bekannten Namen aus Industrie und Handel, Versorger und Entsorger, Unternehmen der Versicherungsbranche, Finanzdienstleister, Reise- und Logistikunternehmen, Verbände, Vereine und Institutionen der öffentlichen Hand. Anwendungen wie Postzustellungsaufträge (PZA/PZU), Wahlbenachrichtigungen, Lohnsteuerkarten, Kontoauszüge, Gehaltsabrechnungen, Inkassoschreiben, Rechnungen und Mahnungen sind dazu nur einige Beispiele.

Jeder Mitarbeiter der iab ist außerdem schriftlich den gesetzlichen Bestimmungen nach §§ 5 und 9 BDSG, dem Fernmeldegeheimnis nach § 88 TKG und dem Postgeheimnis nach § 39 PostG verpflichtet. Ihm ist untersagt, personenbezogene Daten unbefugt zu verarbeiten, zu nutzen oder in irgendeiner Form fremden Personen zugänglich zu machen.

Die internet access GmbH ist seit dem 01. März 2007 nach dem Qualitätsmanagementsystem DIN EN ISO 9001:2000 zertifiziert. Die Zertifizierung für DV-Freimachung mittels eigener Softwarelösung erfolgte bereits im Jahr 2003. Seit Dezember 2012 ist die internet access GmbH nach DIN EN ISO 9001:2008 rezertifiziert.

Unsere Datenschutzverpflichtungen und -bestimmungen im Detail:

**1. Personenbezogene Daten**

Mit unserem Internetauftritt bieten wir Ihnen die Möglichkeit der Kontaktaufnahme an dafür vorgesehenen Stellen an. Die Bearbeitung Ihres Anliegens setzt die Speicherung Ihrer personenbezogenen Daten durch die iab - internet access GmbH voraus. Die hierbei übermittelten Daten werden nur für den Zweck verwendet, für den sie uns überlassen wurden. Eine Weitergabe Ihrer Daten an Dritte erfolgt nicht, außer Sie haben ausdrücklich Ihr Einverständnis dazu erklärt oder aber gesetzliche Vorschriften verpflichten uns dazu. Im Übrigen gelten die gesetzlichen Datenschutzbestimmungen und nachstehenden Verfahren:

**2. online-Datenübertragung/Datensicherheit**

Die Datenübertragung zum Produktionszentrum erfolgt online verschlüsselt und automatisiert. Ein Benutzereingriff in den Produktivbetrieb ist nicht möglich, die Daten sind verschlüsselt und schreibgeschützt und die Mitarbeiter für die Verarbeitung personenbezogener Daten sind nach den gesetzlichen Bestimmungen gemäß § 5 BDSG, nach dem Fernmeldegeheimnis gemäß § 88 TKG und nach dem Postgeheimnis gemäß § 39 PostG verpflichtet. Sämtliche übermittelten Briefdaten werden nach Produktionsabschluss und Übernahme der anonymisierten Daten in das Rechnungsprogramm nach einem Monat gelöscht, es sei denn, der Kunde macht andere Vorgaben. Adressen der Briefempfänger werden nur zur Erstellung der Briefe gespeichert, nicht an Dritte weitergegeben und sind vor unbefugten Zugriff gesichert. Protokolldaten der Produktion werden bereits nach einem Monat gelöscht. Spätestens vier Jahre nach Einspeicherung werden die Datenbestände auf Löschung überprüft. Daten mit steuerlicher Relevanz werden nach fünf Jahren archiviert und nach zehn Jahren gelöscht.

Für Datensicherheit sorgen Firewall, Viren-, Server- und Systemüberwachung, mehrmals tägliche vollautomatische Datensicherung auf getrennten Servern und nach Produktionsabschluss die Vernichtung der Einlieferungsdaten/Belege nach §§ 5 und 9 BDSG. Der Zugang zu sicherheitsrelevanten Zonen erfolgt nur über personalisierte Mitarbeiter-Chipkarten. Wachschutz, Notstrom-, Warn- und Alarmanlagen, Videoüberwachung in den Gebäuden und Produktionszentren ergänzen unsere Sicherungsmaßnahmen und Vorgaben.

**3. Datenschutzverpflichtungen und -bestimmungen**

Der datenverarbeitende und produktionsausführende Dienstleister, die iab - internet access GmbH - Partner Deutsche Post AG, ist dem Datenschutz verpflichtet nach den datenschutzrechtlichen Vorgaben und den gesetzlichen Bestimmungen nach §§ 5 und 9 BDSG, dem Fernmeldegeheimnis des Telekommunikationsgesetzes nach § 88 TKG sowie dem Briefgeheimnis der Deutschen Post AG nach § 39 PostG und erfüllt ebenso die Datenschutzbedingungen des öffentlichen Dienstes, z. B. der Oberfinanzdirektion. Jeder Mitarbeiter der FP IAB - internet access GmbH ist gemäß § 5 BDSG uneingeschränkt auf die Einhaltung des Datengeheimnisses schriftlich verpflichtet. Ihm ist untersagt, personenbezogene Daten unbefugt zu verarbeiten, zu nutzen oder in irgendeiner Form fremden Personen zugänglich zu machen.

**4. Verpflichtungserklärung zum Datenschutz**

Gemäß § 1 des Gesetzes über die förmliche Verpflichtung nicht beamteter Personen (VerpflG in der jeweils gültigen Fassung gemäß BGBl I vom 2. März 1974, 469, 547) und nach Bundesdatenschutzgesetz (BDSG) verpflichtet sich FP IAB - internet access GmbH im Rahmen ihres Auftrages der bestehenden Geschäftsbeziehungen und jeweils gestellten Aufgaben, ihre Obliegenheiten gewissenhaft zu erfüllen.

Der Verpflichteten ist der Inhalt der folgenden Strafvorschriften des Strafgesetzbuches bekannt:

| | |
|---|---|
| § 95 | Offenbaren von Staatsgeheimnissen |
| § 96 | Landesverräterische Ausspähung, Auskundschaften von Staatsgeheimnissen |
| § 97 | Preisgabe von Staatsgeheimnissen |
| § 97b Abs. 2 i. V. m. §§ 94-97: | Verrat in irriger Annahme eines Staatsgeheimnisses |
| § 133 Abs. 3 | Verwahrungsbruch |
| § 201 Abs. 3 | Verletzung der Vertraulichkeit des Wortes |
| § 203 Abs. 2, 4, 5 | Verletzung von Privatgeheimnissen |
| § 204 | Verwertung fremder Geheimnisse |
| § 331, 332 | Vorteilsannahme und Bestechlichkeit |
| § 353b | Verletzung des Dienstgeheimnisses |
| § 355 | Verletzung des Steuergeheimnisses |
| § 358 | Nebenfolgen |

Der Verpflichteten ist weiterhin bekannt, dass die vorgenannten Strafvorschriften aufgrund der Verpflichtung für sie anzuwenden sind. Es gilt das Bundesdatenschutzgesetz in der jeweils gültigen Fassung (gemäß BGBl I Nr. 3 vom 24. Januar 2003). Gemäß § 5 BDSG und § 88 TKG verpflichtet sich die FP IAB - internet access GmbH, das Datengeheimnis uneingeschränkt zu wahren.

Der Verpflichteten ist bekannt, dass es untersagt ist, personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen, und dass diese Verpflichtung auch nach Beendigung der Tätigkeit fortbesteht. Die FP IAB - internet access GmbH trifft daher die technischen und organisatorischen Maßnahmen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Die FP IAB - internet access GmbH versichert, dass ihre Mitarbeiter über den Inhalt der vorgenannten Bestimmungen unterrichtet sind und hat sich dies von Ihnen schriftlich bestätigen lassen.

Über die oben genannten Verpflichtungen hinaus gewährleistet die FP IAB - internet access GmbH verbindlich, keinen Adresshandel zu betreiben und mit keinem Unternehmen des Direktmarketings oder deren Dachorganisationen diesbezüglich in Verbindung zu stehen.

Auf Anfrage können separate Datenschutzvereinbarungen sowie Zusatzvereinbarungen getroffen werden. Aufgrund aktueller Gegebenheiten, wie z. B. bei einer Novellierung des Bundesdatenschutzgesetzes, werden wir falls nötig, diese Datenschutzerklärung aktualisieren.

# Technische und organisatorische Maßnahmen

**zur Umsetzung und Einhaltung der Vorgaben des Bundesdatenschutzgesetzes und weiterer datenschutzrechtlicher Vorgaben**

## 1. Zutrittskontrolle

Die FP IAB - internet access GmbH arbeitet zurzeit an zwei Standorten auf dem WISTA Campus in Berlin-Adlershof. Zum einen befinden sich das Produktionszentrum und die Verwaltung in der Barbara-McClintock-Straße (BMC) und zum anderen arbeiten der Vertrieb und IT Software & Entwicklung in der Albert-Einstein-Straße (AE).

Die Produktion (BMC) ist durch eine Zugangssperre (Terminal ES 335 von Siemens) gesichert. Nur Personen mit gültigem Firmenausweis können das Gebäude betreten. Betriebsfremde Personen haben keinen Zutritt zu Daten verarbeitenden oder produzierenden Zonen. Die gesicherten Zugänge sind über einen Kartenleser und eine Klingel mit Gegensprechanlage für Betriebsfremde (bspw. Lieferanten) verfügbar. Das Gebäude ist durch eine Alarmanlage mit Kameras, Blitzanlage und einer Telefonleitung zum Sicherheitsdienst geschützt, zusätzlich fährt ein privater Wachschutz Streife. In der AE kann das Gebäude nachts nur durch einen passenden Büroschlüssel betreten werden, und es gibt ebenfalls einen privaten Wachschutz, welcher regelmäßige Streifengänge durchführt. Unbesetzte Büros sind verschlossen: Es gibt einen durch einen Mitarbeiter stets besetzten Haupteingang.

## 2. Zugangskontrolle

Identifizierung aller Benutzer und Datenstationen im System sowie Zugangsregelungen und Benutzerberechtigungen sind im Einsatz.

Jeder Mitarbeiter der FP IAB - internet access GmbH ist schriftlich den gesetzlichen Bestimmungen des Bundesdatenschutzgesetzes und allen einschlägigen datenschutzrechtlichen Vorgaben nach §§ 5 und 9 BDSG, dem Fernmeldegeheimnis nach § 88 TKG und dem Briefgeheimnis der Deutschen Post nach § 39 PostG verpflichtet. Als Dienstleister für öffentliche Sektoren bestehen Zusatzvereinbarungen und individuelle Verpflichtungen, wie beispielsweise gegenüber den OFD (nach Prüfung und Anforderung können mit dem Kunden individuelle Zusatzvereinbarungen getroffen werden, sofern die Voraussetzungen der internet access GmbH erfüllt werden können).

Entsprechend den ISO 9001 Anforderungen ist die Perforce Versionsverwaltung mit 8 Lizenzen als unterstützendes Tool im Einsatz.

## 3. Zugriffskontrolle

Funktions- und Zugriffsberechtigungen sowie Ausweisleser sind im Einsatz und werden protokolliert. Zugriffsregelungen, Richtlinien der Dateiorganisation, Protokollierung sind für jeden Standort vorhanden. Mitarbeiter (Benutzer) haben keine Rechte, um Programme zu installieren oder zu nutzen ohne Absprache mit den Administratoren. Personenbezogene Rechte auf jedem Rechner (Einteilung nach Administrator, Benutzer etc.) sowie Verschlüsselungssoftware wie Flam, PGP und andere werden u.a. in Absprache mit den jeweiligen Kunden eingesetzt.

Datenträger mit Firmen- oder Kundendaten auf Papier oder elektronisch werden generell zur Datenmüllvernichtung an ein zertifiziertes Unternehmen (Berlin Recycling GmbH nach Stufe 3 und LWB Lichtenberger Behindertenwerkstatt nach Stufe 4) übergeben, so dass kein Zugriff und Missbrauch von Dritten möglich ist.

## 4. Weitergabekontrolle

Zugangskontrolle nur für befugte Personen, Datenübermittlung erfolgt grundsätzlich elektronisch, daher ist keine Datenträgerverwaltung notwendig. Arbeitsstationen sind ohne Diskettenlaufwerke oder Brenner, so dass keine Kopien angefertigt werden können.

Die elektronische Übermittlung wird immer protokolliert, ist passwortgebunden und nur als automatischer Prozess ohne Benutzereingriff im Produktivbetrieb möglich. Datenübertragungen zwischen den beiden Standorten der FP IAB erfolgen über VPN-Tunnel. Eine Firewall sorgt für die Abwehr von unberechtigten Zugriffen aus dem Telekommunikationsnetz.

Die Postauflieferung wird durch Bring- und Hol-Dienste der DPAG sowie auf Kundenwunsch durch Alternativen Zustelldiensten gewährleistet. Plausibilitäts- und Vollständigkeitsprüfungen erfolgen anhand von Service-Data-Line Verfahren, mehrstufigen Arbeitslaufzetteln mit elektronischem Abgleich sowie durch Barcode- und Data-Matrix-Leseverfahren für Produktionsparameter.

**5. Eingabekontrolle**

Die Eingabekontrolle erfolgt anhand der Verfahrens-, Programm- und Arbeitsablauforganisation nach ISO 9001 und gibt Auskunft über den Mitarbeiter und die Anwendung der jeweiligen Produktion.Personenbezogen Daten werden nicht erfasst, diese werden vom Auftraggeber gestellt. Die Datenverarbeitung läuft automatisiert.

**6. Auftragskontrolle**

Interne Kontrollen werden ausgeführt mittels formalisierter Serviceverträge, SLA´s, Produktionsvereinbarungen, jobbezogenen Produktionsreports (Track & Trace in Vorbereitung), Formalisierte und elektronisch überwachte Auftragslaufzettel, automatisch erzeugte und geprüfte DV-Freimachungslisten, BZE-/BZA-Einlieferungslisten und sonstigen Nachweise. Der Auftraggeber hat die Möglichkeit das Sicherheitskonzept zu überprüfen und die Produktionsräumlichkeiten nach Ankündigung zu besichtigen.

**7. Verfügbarkeitskontrolle**

Alle Daten werden durch tägliche mehrstufige Backups gesichert. Wichtige Server werden dupliziert oder in Raid Konfigurationen betrieben. Alle Produktionsrechner und -verfahren werden zusätzlich auf Backup Rechnern in den aktuell gültigen Konfigurationen vorgehalten, die als Standby Production Devices innerhalb von 15 Minuten produktiv gesetzt werden können, so dass eine optimale Hochverfügbarkeit auch auf Anwendungsebene gegeben ist.

**8. Zweckbindungskontrolle/Trennungsgebot**

Die zweckgebundene Mandanten- und Funktionstrennung ist vollständig sichergestellt. Die Trennung der zu unterschiedlichen Zwecken erhobenen Daten wird durch getrennte Speicherung, durch logische Trennung über Kundenverzeichnisse mit unterschiedlichen Zugriffsberechtigungen und zweckgebundene Kennzeichnungen und Ablagestrukturen der jeweiligen Datenanwendungen realisiert. Für die Dateneinlieferung erhält der Kunde einen eigenen Kundenaccount mit Logindaten (Benutzernamen und Passwort).

**9. Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag (§ 11 BDSG)**

(1) Werden personenbezogene Daten im Auftrag durch FP IAB erhoben, verarbeitet oder genutzt, ist FP IAB auch für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz, wie dem Fernmeldegeheimnis des Telekommunikationsgesetzes, verantwortlich.

(2) Unter besonderer Berücksichtigung der Eignung der von FP IAB getroffenen technischen und organisatorischen Maßnahmen wird der Auftrag schriftlich erteilt, wobei insbesondere im Einzelnen festzulegen sind:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 9 zutreffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die nach Absatz 4 bestehenden Pflichten von FP IAB, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten von FP IAB,
8. mitzuteilende Verstöße von FP IAB oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber FP IAB vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung bei FP IAB gespeicherter Daten nach Beendigung des Auftrages.

Der Auftrag kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden. Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der bei FP IAB getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

(3) FP IAB darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(4) Für FP IAB gelten neben den Vorschriften des BDSG §§ 5, 9, 43 Abs. 1 Nr. 2, 10 und 11, Abs. 2 Nr. 1 bis 3 und Abs. 3 sowie § 44 auch der § 88 TKG und die Vorschriften über die Datenschutzkontrolle und -aufsicht.

(5) Die Absätze 1 bis 4 gelten entsprechend, wenn externe Personen z.B. bei Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen, wie bspw. Wartungsfirmen, im Auftrag vorgenommen werden. Diese Personen werden ebenso mit einer Erklärung zum Datenschutz nach § 5 BDSG und § 88 TKG verpflichtet.