



1. Grundsatz

Die ibu gmbh orientiert sich in ihrer Arbeit grundsätzlich an den geltenden Datenschutzbestimmungen. Dies umfasst im Einzelnen die folgenden Punkte:

1.1 Verpflichtung der Mitarbeiter*innen

Alle Mitarbeiter*innen werden über die datenschutzrechtlichen Regelungen informiert und zur Einhaltung dieser Regelungen verpflichtet. Jährlich werden die Mitarbeiter*innen auf ihre Verpflichtung zur Einhaltung der Regelungen hingewiesen.

1.2 Informationen und Schulungen zum Datenschutz

Die ibu gmbh trägt dafür Sorge, dass die Mitarbeiter*innen die zur Durchführung der spezifischen Aufgaben notwendigen Kenntnisse und Erfahrungen besitzen. Soweit projektspezifische sachliche oder methodische Kenntnisse insbesondere zum Datenschutz erforderlich sind, werden diese den Mitarbeiter*innen in Schulungsmaßnahmen vermittelt.

2. Umgang mit Erhebungsunterlagen

2.1 Aufbewahrung und Zugang

Personenbezogene Unterlagen werden in verschließbaren Schränken/Räumen projektbezogen aufbewahrt und ausschließlich zum Zwecke der elektronischen Datenerfassung und zur Bearbeitung oder zu Prüfungszwecken herausgenommen. Der Zugang zu den projektbezogen aufbewahrten Unterlagen ist lediglich autorisierten Mitarbeiter*innen des jeweiligen Projektes gestattet.

2.2 Zeitnahe Verarbeitung

Erhebungsunterlagen (z.B. Fragebögen, Erhebungsbögen etc.) werden zeitnah nach Eingang ggf. elektronisch weiterverarbeitet.

2.3 Aufbewahrungen nach Abschluss

Um Fragen auch nach Abschluss der Maßnahmen beantworten zu können, werden dafür Mindestzeiträume für die Aufbewahrung festgelegt. Nur dem Bereichsleiter oder den Mitarbeiter*innen ist der Zugriff auf die Unterlagen erlaubt. Nach Ablauf der Aufbewahrungszeit werden die zu einem Projekt gehörigen Unterlagen unter persönlicher Aufsicht des Projektleiters oder eines/r Projektmitarbeiters/in vernichtet.

3. Datenerfassung, Datenanalyse und Archivierung

3.1 Zugang zu eingesetzten Rechnern

Die Administration der Rechner obliegt der ibu gmbh und dem/r Datenschutzbeauftragten. Alle im institutseigenen Netzwerk vorhandenen Rechner sind mit einem Passwort geschützt. Der Zugang zu diesen Rechnern ist ausschließlich dem jeweiligen Mitarbeitern erlaubt.



3.2 Passwortverwaltung

Die Passwörter sind ausschließlich dem Geschäftsführer sowie den förmlich verpflichteten Mitarbeiter*innen bekannt. Der/die Bereichsleiter/in erfasst schriftlich, welche Mitarbeiter*innen über welche Passwörter informiert sind.

3.3 Aufbewahrung der Sicherungskopien

Die Sicherungskopien werden in einem verschlossenen Schrank aufbewahrt.

3.4 Datennutzung

Der Umgang mit den elektronisch erfassten Daten ist ausschließlich dem/der zuständigen Bereichsleiter/in und autorisierten Mitarbeiter*innen gestattet.

4. Umgang mit personenbezogenen Daten

4.1 Erhebung personenbezogener Daten

Personenbezogene Daten (Namen, Adressen, Kommunikationsverbindungen sowie alle Angaben, die eine Zuordnung von Einzelpersonen zu Daten ermöglichen) werden ausschließlich dann erhoben und/oder auf Datenträgern erfasst, wenn dies begründet ist.

4.2 Erfassungsmedien

Auf Tonträgern werden grundsätzlich keine personenbezogenen Daten erfasst.

4.3 Datenvernichtung

Personenbezogene Daten werden zum frühestmöglichen Zeitpunkt gelöscht bzw. vernichtet.

4.4 Nutzung personenbezogener Daten

Soweit in einem Projekt personenbezogene Daten erhoben und weiterverarbeitet werden, ist der Umgang mit diesen Daten ausschließlich dem/der Bereichsleiter/in und den schriftlich dazu autorisierten Mitarbeiter*innen gestattet. Eine Liste der Personen, die mit personenbezogenen Daten umgehen, wird der Datenschutzbeauftragten schriftlich vorgelegt.

4.5 Passwortschutz personenbezogener Daten

Dateien mit personenbezogenen Daten, die während der Bearbeitungsphase auf einem Rechner gespeichert sind, werden durch ein nur dem/der Bereichsleiter/in oder autorisierten Mitarbeiter*innen bekanntes Passwort geschützt.

4.6 Vernichtung personenbezogener Unterlagen

Der/die Bereichsleiter/in und die autorisierten Mitarbeiter*innen sind für eine datenschutzgerechte Vernichtung nicht mehr benötigter Ausdrucke von personenbezogenen Daten sowie anderer nicht mehr benötigter personenbezogener Unterlagen verantwortlich.



4.7 Veröffentlichung personenbezogener Daten

Es erfolgt keine Veröffentlichung personenbezogener Daten. Ausnahmen sind nur dann zulässig, wenn eine Einwilligung des/der Betroffenen zur Veröffentlichung vorliegt.

5. Umgang mit Akten

5.1 Verschluss des Aufbewahrungsortes

Die Aktenschränke sind (außer zur Ausgabe oder Hineingabe von Akten) verschlossen. Die Schlüssel werden von dem/der Bereichsleiter/in oder einem der förmlich verpflichteten Mitarbeiter*innen verwahrt.

5.2 Bearbeitung von Akten

Der Umgang mit Akten ist ausschließlich auf Mitarbeiter*innen beschränkt, die auf das Datengeheimnis verpflichtet wurden. Jedem/r Mitarbeiter/in ist es ausschließlich erlaubt, Akten für das Projekt, in dem er/sie tätig ist, zu entnehmen. Es wird immer nur die Anzahl von Akten dem Aufbewahrungsschrank entnommen, die bearbeitet werden. Es ist untersagt, Akten unbeaufsichtigt in den Arbeitsräumen liegen zu lassen. Unmittelbar nach Abschluss der Bearbeitung werden die entnommenen Akten durch den/die Bereichsleiter/in oder einen der förmlich verpflichteten Mitarbeiter*innen wieder an ihren Platz im verschließbaren Schrank gelegt und verschlossen.

5.3 Vertraulichkeit und Verschwiegenheit

Alle Informationen, die die ibu gmbh vom Auftraggeber erhält, werden streng vertraulich behandelt. Sie werden Dritten nicht zugänglich gemacht.

Neustadt-Glewe, den 09.03.2021

Chr. Rosenkranz
Geschäftsführer