Datenschutz-Compliance-Richtlinie der DATABAU Unternehmensgruppe

1. Präambel:
Diese Datenschutz-Compliance-Richtlinie setzt die Verpflichtung des Unternehmens um, personenbezogene Daten gemäß den geltenden Datenschutzgesetzen, wie der Europäischen Datenschutz-Grundverordnung (DSGVO), dem Bundesdatenschutzgesetz (BDSG) sowie weiteren relevanten Vorschriften, zu schützen und zu verarbeiten.

2. Geltungsbereich:
Die Richtlinie gilt für alle Mitarbeiter, Abteilungen, Geschäftsbereiche und Tochtergesellschaften der Unternehmensgruppe, die personenbezogene Daten verarbeiten.

3. Ziele:
Das zentrale Ziel dieser Richtlinie ist es, die Einhaltung der Datenschutzbestimmungen sicherzustellen, das Bewusstsein und Verständnis für Datenschutzfragen im Unternehmen zu erhöhen und Risiken im Zusammenhang mit Datenschutzverletzungen zu minimieren.

4. Verantwortlichkeiten:
- Unternehmen: Jede Gesellschaft der DATABAU Unternehmensgruppe ist datenschutzrechtlich für sich verantwortlich.
Geschäftsführung: Hat die oberste Verantwortung für die Einhaltung dieser Richtlinie in ihrer Gesellschaft.
- Datenschutzbeauftragter: Ist verantwortlich für die Überwachung der Einhaltung der Richtlinie, die Beratung und Schulung der Mitarbeiter sowie die Berichterstattung an die Geschäftsführung in seiner Gesellschaft.
- Mitarbeiter: Sind verpflichtet, diese Richtlinie zu befolgen und bei Datenschutzverstößen oder Unklarheiten den Datenschutzbeauftragten zu informieren.

5. Grundprinzipien:
- Rechtmäßigkeit: Personenbezogene Daten dürfen nur verarbeitet werden, wenn eine gesetzliche Rechtsgrundlage oder eine Einwilligung vorliegt.
- Transparenz: Die betroffene Person muss über die Verarbeitung ihrer Daten informiert sein gemäß Art. 13 und 14 DSGVO. Dies gilt für alle Personen, deren Daten verarbeitet werden, also insbesondere für Mitarbeiter, Geschäftspartner und Bewerber.
- Zweckbindung: Daten dürfen grds. nur für den festgelegten und legitimen Zweck, für den sie erhoben wurden, verarbeitet werden.
- Datenminimierung: Es dürfen nur so viele Daten wie nötig verarbeitet werden.
- Richtigkeit: Es ist sicherzustellen, dass Daten korrekt und aktuell sind.
- Speicherbegrenzung: Daten dürfen nicht länger als nötig gespeichert werden.
- Integrität und Vertraulichkeit: Die Sicherheit der Daten muss durch geeignete technische und organisatorische Maßnahmen gewährleistet werden.
- Rechenschaft: Jede Gesellschaft kann die Einhaltung dieser Grundprinzipien nachweisen.

6. Verarbeitungsaktivitäten:
Jede Verarbeitung personenbezogener Daten muss geprüft und im

Verarbeitungsverzeichnis dokumentiert werden, um ihre Konformität mit den Datenschutzprinzipien sicherzustellen. Die Erforderlichkeit von Datenschutz-Folgenabschätzungen wird bewertet und das Ergebnis wird dokumentiert. Soweit rechtlich erforderlich werden Datenschutz-Folgenabschätzungen gemäß Art. 35 DSGVO durchgeführt.

7. Datenschutzvorfälle:
Datenschutzvorfälle nach Art. 33 DSGVO müssen umgehend gemeldet und entsprechend dokumentiert werden. Die Meldung erfolgt an den Datenschutzbeauftragten, der über das weitere Vorgehen entscheidet. Soweit rechtlich erforderlich, erfolgt eine Meldung an die zuständige Aufsichtsbehörde und eine Information der Betroffenen (Art. 34 DSGVO).

8. Schulung und Bewusstsein:
Alle Mitarbeiter müssen regelmäßig bedarfsgerecht zu Datenschutzthemen geschult werden und Zugang zu Ressourcen und Unterstützung im Zusammenhang mit Datenschutz erhalten. Alle Mitarbeiter werden auf die Einhaltung des Datenschutzes verpflichtet.

9. Datenschutzrechtliche Vereinbarungen:
Beim Einsatz von externen Dienstleistern und der Zusammenarbeit mit externen Stellen werden soweit erforderlich Verträge zur Auftragsverarbeitung (Art. 28 DSGVO) oder zur gemeinsamen Verantwortlichkeit (Art. 26 DSGVO) geschlossen.

10. Überwachung und Überprüfung:
Die Einhaltung dieser Richtlinie wird regelmäßig überwacht und überprüft. Festgestellte Mängel werden umgehend behoben. Zuständig ist der Datenschutzbeauftragte und/oder die Geschäftsführung der jeweiligen Gesellschaft.

11. Sanktionen:
Verstöße gegen diese Richtlinie können disziplinarische Maßnahmen durch den Arbeitgeber nach sich ziehen, bis hin zur Kündigung. Zudem sind auch Bußgelder durch Datenschutzaufsichtsbehörden gegen Unternehmen oder Einzelpersonen möglich, ebenso wie strafrechtliche Verurteilungen und Schadensersatzansprüche.