Datenschutz-Spickzettel

Wenn Informationen über natürliche Personen, egal ob sensibel oder nicht, in irgendeiner Weise erfasst gespeichert oder genutzt werden:	*Kontaktdaten von Ansprechpartnern bei Kunden (B2B) in CRM (Kundendatenbank) speichern, Newsletter an Kunden versenden, Bestellung von Server betreiben, gesprächen in rmationen von en*

Für alle Mitarbeit

1	Daten nur in der und nutzen [→ 5 ist	
	a) zur Vertragsabwicklung, oder	*Kontoverbindung der Mitarbeiter zur Gehaltsauszahlung nutzen*
	b) zur Erfüllung von Gesetzen, oder	*Identifikationsdaten von Vertragspartnern gemäß Geldwäschegesetz abfragen und speichern*
	c) das Unternehmen gute Gründe hat und aus Sicht der Betroffen nichts dagegen spricht, insbesondere diese damit rechnen mussten	*geschäftliche Unterlagen eines erkrankten Mitarbeiters Einsehen, um dringende Kundenanfrage zu bearbeiten*
	d) die Betroffenen eindeutig und informiert zugestimmt haben [→ 6.3]	*Mitarbeiter erlaubt Nutzung seines Portraits im Intranet, Kunde bestellt Newsletter*
2	Daten zu Gesundheit und Religion und andere **sensible Daten** überhaupt nicht erfassen und verwenden, außer dies ist ausnahmsweise zulässig. [→ 6.2]	*Krankheitsfehlzeiten, Religionszugehörigkeit, Angaben über sexuelle Orientierung*
3	Daten nur für die **Zwecke** verwenden, für die sie ursprünglich gesammelt wurden. [→ 5.1.3]	*Zur Datensicherheit gespeicherte Login- und Logout-Zeiten von Mitarbeitern nicht zur Arbeitszeitkontrolle nutzen.*
4	**Nicht mehr Daten** erfassen und nutzen als für den konkreten Zweck nötig (keine Speicherung auf Vorrat). [→ 5.1.4]	*Die Abfrage von Namen und Arbeitgeber ist für die Zusendung von Newslettern nicht nötig.*
5	Daten **löschen**, wenn sie nicht mehr benötigt werden. [→ 5.1.6]	*Bewerbungen abgelehnter Kandidaten spätestens 6 Monate nach der Auswahlentscheidung löschen.*
6	Unrichtige oder unvollständige Daten **korrigieren** [→ 5.1.5]	*In Dokumentation zum Mitarbeitergespräch nicht protokollierte Bedenken des Betroffenen ergänzen.*
7	Bei **Unklarheiten** den **Datenschutzbeauftragten fragen**, sofern benannt. [→ 3.5, 4]	*Gilt für IP-Adressen der Datenschutz?*
8	Wenn Unbefugte Zugang zu Daten erhalten haben, Daten verloren gegangen bzw. nicht mehr verfügbar	*Verlust oder Diebstahl eines Notebooks, Smartphones oder USB-Sticks, Hackerangriff auf*