Datenschutzdeklaration zur IT-Ziviltechniker & Sachverständigentätigkeit

IT-Ziviltechniker und Gerichts-Sachverständiger
DDipl.-Ing. Mag. Gernot Schmied
iwF. auch als „SV“ abgekürzt

Stand 24.08.2024

Einleitung

Im Rahmen der beruflichen Tätigkeit, Projekten und insbesondere forensischer Ermittlungen und Untersuchungen kommt der SV naturgemäß in Berührung mit vertraulichen, personenbezogenen oder gar personen-sensiblen Daten, dafür stellt der SV diese **Datenschutzdeklaration** bei. Wünscht ein Kunde eine über diese Deklaration hinaus gehende **Datenverarbeitungsvereinbarung**, werden die für die Abstimmung anfallenden Kosten in Rechnung gestellt.

Als SV respektiere und schütze ich das Recht auf Datenschutz und Privatsphäre und ergreife alle gesetzlich erforderlichen Maßnahmen, um personenbezogenen Daten zu schützen:

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten betroffener Personen treffe ich geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung *(„Verfügbarkeit, Integrität und Vertraulichkeit“*).

Datenschutzrechtliche Rolle von Sachverständigen bei Gutachtensaufträgen

Die Sachverständigentätigkeit wird in Personalunion als IT-Ziviltechniker und Gerichts-SV ausgeübt. Strenge Verpflichtungen hinsichtlich **Vertraulichkeit und Verschwiegenheit** resultieren grundsätzlich aus dem **SDG, ZTG sowie den jeweiligen Standesregeln**. Diskretion ist für mich oberstes Gebot, es gibt keinerlei Auskünfte zu Referenzprojekten noch Interviews.

Als SV bediene ich mich bei Bedarf offengelegter hochqualifizierter Dritte als Werkvertragsnehmer oder arbeite auf Wunsch von Auftraggebern mit von Ihnen namhaft gemachten Experten zusammen, insbesondere mit Juristen. Fest-angestellte Dienstnehmer gibt es nicht.

Datenschutzrechtlich sind SV im Rahmen ihrer Gutachtenstätigkeit – unabhängig davon, (a) ob sie von einem Gericht bzw. einer Behörde bestellt werden oder (b) ob sie im privaten Auftrag tätig sind – als „**Auftragsverarbeiter**“ zu qualifizieren. Datenschutzrechtlicher „Verantwortlicher“ ist jeweils der „Auftraggeber“, also das jeweilige Gericht, die Behörde bzw. der jeweilige „private“ Gutachtensauftraggeber.

Dementsprechend sind diese – und nicht die SV – insbesondere auch für die Erfüllung der datenschutzrechtlichen Betroffenenrechte, wie insbesondere etwaiges Recht auf Information, Auskunft, Richtigstellung, Löschung, Einschränkung, Datenübertragung und/oder Widerspruch, berufen. Sämtliche Anträge zu Betroffenenrechten sind daher direkt beim Gericht/bei der Behörde bzw. dem „privaten“ Gutachtensauftraggeber und nicht bei den (Gerichts)SV geltend zu machen. Sollten Anträge doch bei den (Gerichts)SV gestellt werden, werden diese an den jeweiligen datenschutzrechtlichen Verantwortlichen weitergeleitet.

Insbesondere die **datenforensische SV-Tätigkeit** ist dahingehend besonders, dass zu Beginn der Untersuchungen meist unklar ist, was vorgefunden wird und welche Schritte zur Beantwortung von Gutachtensfragen erforderlich

sind. Eine minimalinvasive Vorgehensweise ist stets Gegenstand der Abstimmung, ebenfalls Regelungen zu offensichtlichen privaten Daten und zum Umgang mit Zufallsfunden.

Aus Datenschutzgründen wurde auf die Verwendung von **E-Mail-Marketing** völlig verzichtet, dieses erfolgt ausschließlich über Business Social Networks Xing und LinkedIN.

Organisatorische Maßnahmen:

- **Transparenz:** Keine Hinzuziehung von Dritten ohne Offenlegung der Qualifikation und vorherige Rücksprache mit dem gerichtlichen oder privaten Auftraggeber.
- **Qualität:** Auswahl hochwertiger, verlässlicher und langjährig erfahrener und dem SV bekannter Erfüllungsgehilfen oder Hilfsgutachter. Es erfolgt eine ständige Überwachung der Tätigkeiten und Fortschritte.
- **Datenübermittlung** erfolgt über verschlüsselte Kanäle oder Datenträger, alternativ **Datenbereitstellung** über sichere Datenräume. Das Verfahren ist mit dem Auftraggeber bei Beauftragung abzustimmen.
- Lückenlose Weitergabeverfolgung von datenforensischen Sicherstellungen erfolgt über ***Chain of Custody*** **Formular** (Wahrung der Beweiskette).
- Es erfolgt grundsätzlich **kein Versand von Datenträgern**, sondern immer persönliche Übergabe und Entgegennahme. Ist dies nicht möglich, erfolgt Versand durch hochwertige Kurierdienste und in verschlüsselter Form nach Maßgabe der mengenbedingten Möglichkeiten. Das Untergangs- und Verlustrisiko trägt der Auftraggeber, der dem Verfahren explizit zuzustimmen hat.
- Alle ursprünglichen Beweismitteldaten (i.d.R. forensische Datenträgerkopien oder forensische Abbild-Dateien) sowie die zugehörige Falldatenbank werden nach vollständigem **Abschluss des Gutachtensauftrags** und nach schriftlicher Bestätigung des Auftraggebers zum festgelegten Zeitpunkt von den Systemen des SV gelöscht.

Technische Maßnahmen

- Vollständige Microsoft Bitlocker-Datenverschlüsselung auf allen mobilen Geräten und Datenträgern als Schutz gegen Diebstahl und Verlust und zur Erleichterung des Ausrangierens bei Untergang.
- Datenforensik: Verschlüsselung von Übergabedatenträgern und Einsatz verschlüsselter Images im Ermessen des Sachverständigen und abhängig von Datenmenge den Möglichkeiten des Empfängers, um die Weiterverarbeitbarkeit und Importe sicherzustellen.
- Verschlüsselung der festen Laborinfrastruktur nach Maßgabe der Möglichkeiten, da Performance- und Stabilitätsanforderungen und schierer Umfang dem entgegenstehen. Es gelangen durchgängig RAID-1 und RAID-10 Konfigurationen zum Einsatz.
- Die Herausforderung von defekten Datenträgern wird bei Neuanschaffungen ab 2021 mittels self-encrypting devices (SEDs) gelöst, die moderne Verschlüsselungs- und Löschstandards unterstützen. Zusätzlich oder alternativ erfolgt mechanische Unbrauchbarmachung oder forensische Mehrfachlöschung *lege artis*.
- Sofern Cloud-Datenablagen zum Einsatz gelangt, erfolgt dies nach Maßgabe der Möglichkeiten verschlüsselt in Ablage (*data@rest*) und Übermittlung (*data-in-motion*) oder alternativ mit Overlay-Verschlüsselung wie z.B. BoxCryptor. Der vom SV verwendete NextCloud Datenraum wird in Deutschland gehostet und durch vorgelagerte Cloudflare WAF (Web Application Firewall) geschützt, eine server-seitig Verschlüsselung ist aus technischen Gründen nicht möglich.
- Die Wordpress Web Page des SV wird ebenfalls durch eine integrierte Wordfence WAF (Web Application Firewall) geschützt.
- Backups wichtiger Daten erfolgen mehrmals täglich in verschlüsselter Form in zwei Cloud-Speicher sowie monatlich auf portable Disk zur Verwahrung in einem Banksafe. Restore Tests erfolgen 2 x jährlich, ebenso die Überprüfung von im Internet erreichbaren Web-Ressourcen und Zertifikaten mit *lege artis* Scan-Werkzeugen.
- Die Sicherheit wird durch ein mehrschichtiges Konzept gewährleistet: Umfassende Cisco Firepower Sicherheits-Infrastruktur incl. Umbrella und EDR, ergänzt um Microsoft Defender Endpoint Protection. Azure und Microsoft 365 Absicherung der Testumgebungen erfolgt mit den dazugehörigen Microsoft Mitteln.

- Ebenso erfolgt eine zweifache SPAM- und Malware-Filterung von Emails. Starke Verschlüsselung von Emails und ZIP-Archiven erfolgt je nach Anforderungen und Möglichkeiten des Auftraggebers in Abstimmung mit diesem. Angeboten wird X.509v3, PGP und starke symmetrische ZIP-Verschlüsselung für Anhänge.
- Einsatz von starker 2-Fakter Authentifizierung wo immer möglich mittels ID-Austria, Authenticator Apps, Yubico Token, Smartcards.