Kammer der
ZiviltechnikerInnen
Steiermark und Kärnten

A-8010 Graz, Schönaugasse 7/1
T +43 (0)316 82 63 44-0
F +43 (0)316 82 63 44-25
office@ztkammer.at, www.ztkammer.at

FAQs aus den Seminaren "Fit für die Europäische Datenschutz Grundverordnung (EU-DSGVO)"

Moderation:

Dipl.-Ing. Peter **SKALICKI-WEIXELBERGER**, Ing. Kons. f. Vermessungswesen, DI Mussack & DI Skalicki-Weixelberger ZT-KG, INNOGEO ZT-KG, Vorsitzender des Ausschusses Daten der Kammer der ZiviltechnikerInnen für Steiermark und Kärnten, Mitglied der E-Government Expert Groups der WKO, Präsident des Österreichischen Dachverbandes für Geographische Informationen (AGEO), Graz

Referenten:

RA Dr. **Rainer BECK**, MMag.art., selbständiger Rechtsanwalt, Lehrtätigkeit an der Kunstuniversität Graz, Karl-Franzenz-Universität Graz und an der FH Campus 02 zu den Themen Urheber- und Verlagsrecht, Bühnenrecht, Kulturmanagement, Legal Aspects on Internet & Social Media, Urheberrechtsverträge, allgemein beeideter und gerichtlich zertifizierter Sachverständiger für Urheberfragen aller Art, Gutachter für Gerichte sowie private Auftraggeber zu allen urheberrechtlichen Fragen (wie Lizenzen, Plagiate, Digitalisierung von Rechten, Persönlichkeitsrechte), Graz

Dipl.-Ing. Dr.techn. Peter **Anton MANDL**, Ing. Kons. für Telematik, allgemein beeideter und gerichtlich zertifizierter Sachverständiger für Elektrotechnik, Nachrichtentechnik, Informationstechnologien, Elektrische Messtechnik, Arbeit und Betrieb, Sachverständiger am Internationalen Strafgerichtshof (ICC Den Haag), Mitglied der Bundesfachgruppe Informationstechnologie der Bundeskammer der ZiviltechnikerInnen, Graz

Stand: 16.5.2018

DVR 0401307

Eingangs wird explizit darauf hingewiesen, dass bei den bereitgestellten Informationen keinerlei Gewähr für die Aktualität, Korrektheit, Vollständigkeit oder Qualität übernommen werden kann. Diese Informationen ersetzen keine rechtliche Beratung und es können aus der Verwendung der Inhalte auch keine Rechtsansprüche begründet werden!

Im konkreten Anlassfall wenden Sie sich bitte an eine Expertin oder einen Experten.

Aus Gründen der besseren Lesbarkeit wird auf geschlechterspezifische Unterscheidung verzichtet.

Fragenkatalog sortiert nach Themenbereiche:

I. **Fragen zum Thema Schutzbereich/Rechtmäßigkeit der Verarbeitung**
II. **Fragen zur Einwilligungserklärung**
III. **Fragen zum Datenverarbeitungsregister/Risikobewertung**
IV. **Fragen zum Datenschutzbeauftragten**
V. **Fragen zu technisch-/organisatorischen Maßnahmen**
VI. **Fragen betreffend Anträgen von Personen (zB Auskunft, Abändern, Löschen)**
VII. **Gesonderte Fragen aus dem Publikum**

I. Fragen zum Thema Schutzbereich/Rechtmäßigkeit der Verarbeitung

1. Zählen Grundbuchsauszüge, Bestandspläne, projektierte Planungen (private Gebäude, Firmengebäude), Projektunterlagen zu den Daten im Sinne der Datenschutzverordnung?

   Von der EU-DSGVO werden nur personenbezogene Daten umfasst. Darunter werden alle Informationen verstanden, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

   Grundbuchsdaten sind öffentliche Daten und unterliegen nicht der EU-DSGVO. Sollten Daten dieser Art allerdings in einem privaten EDV-System oder analog für eigene Zwecke erfasst bzw. verarbeitet werden, ist der Anwendungsbereich der Verordnung wiederum gegeben, sofern daraus aufgrund Adressen, Eigentümer Rückschlüsse auf Personen möglich sind.

   Planungsunterlagen sind weniger ein Thema des Datenschutzes als vielmehr des Urheberrechts. Befinden sich auf solchen Unterlagen keine personenbezogene Daten, ist der Anwendungsbereich der DSGVO nicht eröffnet.

2. Wie ist mit personenbezogenen Daten auf Projektunterlagen (zB.: Name & Adresse der Bauwerber/Antragsteller auf Plänen & Beschreibungen,…) umzugehen, sind das Daten im Sinne der EU-DSGVO ?

   Ja.

   Sofern es zB eine rechtliche Verpflichtung oder einen Vertrag gibt (z.B. Anrainerverzeichnis etc.), ist keine Einwilligung nötig.

3. Fallen Akten (Projektordner, die personenbezogene Daten wie Namen, Adresse, Kontaktdaten enthalten,…), die nach bürointernen Projektnummern sortiert analog (in Regalen) oder digital (Dateiordner) abgelegt sind, unter die EU-DSGVO ?

   Ja.

   Nach der EU-DSGVO ist es unerheblich, ob personenbezogene Daten digital oder analog verarbeitet werden.

4. Gelten Informationen zum religiösen Bekenntnis in Bewerbungsunterlagen als sensible Daten ?

   Ja.

   Artikel 9 der DSGVO normiert die Verarbeitung von „besonderen Kategorien personenbezogener Daten" („sensible Daten").

   Darunter versteht man jegliche Daten, aus denen die rassische und ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugung oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten oder biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

5. Gelten Bankverbindungen (IBAN/BIC) als sensible Daten ?

   Bankverbindungen sind personenbezogene Daten, allerdings keine „sensiblen Daten"

   Ergänzend siehe Frage 4 (Kapitel I).

6. Fallen Rechnungsordner/Anbotsordner mit Anboten/Rechnungen (adressiert auf personenbezogene Daten), sortiert nach Zeit oder Projektnummer (digital & analog) unter die EU-DSVGO ?

   Ja.

   Daten, mit denen natürliche Personen identifiziert werden können oder identifizierbar sind, fallen bei einer Verarbeitung in den Anwendungsbereich der EU-DSGVO. Anonymisierte Daten sind nicht erfasst.

7. Fallen Aufstellungen, Listen mit Rechnungsinfos, die Kunden (auch privaten Personen) zuzuordnen sind unter die EU-DSGVO ? (Etwa Umsatzlisten, die als Information zwischen Steuerberater & Unternehmen / Behörden dienen und in Ordnern - digital/analog dem Steuerberater oder Finanzämtern zugeordnet sind)

   Ja.

   Hier gilt es, eine eventuelle Kollision zwischen der 7 jährigen Aufbewahrungsfrist iSd § 132 BAO (allenfalls länger als 7 Jahre) und der Löschungsverpflichtung (nicht mehr benötigte Daten sind zu löschen) nach der EU-DSGVO zu beachten. Gesetzliche Aufbewahrungspflichten sind einzuhalten (allenfalls anonymisieren).

8. Muss man im Zuge der Erstellung eines Anrainerverzeichnisses aus der öffentlichen Grundbuchsdatenbank zur Erstellung einer bau- oder gewerberechtlichen Einreichung und dem projektbezogenen Speichern eines solchen Verzeichnisses (mit Name und Anschrift der Grundstückseigentümer) alle Anrainer über diese Erhebung der Daten im Sinne der EU-DSGVO informieren ?

   Die Rechtmäßigkeit einer solchen Datenverarbeitung könnte sich aus Artikel 6 Abs. 1 EU-DSGVO ableiten. Jene Verarbeitungen, die für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, oder zur Erfüllung einer rechtlichen Verpflichtung, erforderlich sind, gelten als rechtmäßig.

   Nach Abschluss des konkreten Anlassfalls müssten allerdings die personenbezogenen Daten gelöscht werden. Eine Information der Anrainer, dass ihre Daten erhoben wurde, sollte dennoch durchgeführt werden.

   Aus heutiger Sicht und mangels ensprechender Judikatur kann keine erschöpfendere Antwort gegeben werden.

9. Sind Lieferanten/Dienstleister (Internet-Provider, Telefonanbieter, Homepage-Ersteller, EDV-Administratoren, App-Anbieter,…) zur Bekanntgabe ihrer Maßnahmen zur EU-DSGVO verpflichtet, kann man solche unentgeltlich einfordern? Muss zum Beispiel ein Unternehmen, das Websites erstellt, bekannt geben, welche Daten (IP-Adressen,…) gespeichert werden ? Muss ein App-Anbieter solche Auskünfte erteilen?

   Wurden Lieferanten/Dienstleister von Ziviltechnikern beauftragt, sind sie Auftragsverarbeiter iSd EU-DSGVO. Den Ziviltechniker als Verantwortlichen trifft bei einer Datenverletzung durch seine Lieferanten/Dienstleister ein Auswahlverschulden. Eine noch sorgfältigere Auswahl von Lieferanten/Dienstleiter ist erforderlich. Die Kunden müssen über Kategorien von Empfängern von Daten informiert werden.

10. Widerspricht das Führen eine Kundendatei (Outlook) zum Versenden von Newslettern, Informationen (Kundeninformationen nach Auftragsabschluss) der Zweckbindung (aus der normalen Auftragsabwicklung) und ist daher für eine solche Verarbeitung eine gesonderte Zustimmungserklärung erforderlich?

    Ja, die Zustimmung ist notwendig für Speichern, Verarbeiten und speziell für etwaiges „Profiling".

11. Stellen Kostenschätzungen, Liegenschaftsbewertungen, die als Grundlage für Entscheidungen zu Kredit- oder Fördervergaben führen, eine Voraussetzung für die Verpflichtung zur Datenschutzfolgeabschätzung dar?

    Wenn die Datenverarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, muss der Verantwortliche vorab eine Abschätzung der Folgen der

vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchführen (Datenschutzfolgeabschätzung).

Eine solche ist insbesondere in folgenden Fällen erforderlich:

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder

c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

In dem konkret angesprochenen Fall müsste nur dann eine Datenschutz-Folgeabschätzung durchgeführt werden, wenn irgendwo ein „hohes Risiko" betreffend dem Schutz von personenbezogenen Daten gegeben ist.

12. Dürfen Fotos/Visualisierungen, Pläne, Beschreibungen von privaten Projekten / Personen anonymisiert (nicht unter Familiennamen, sondern etwa unter einem Projektkürzel oder einer Nummer) ohne schriftliche Zustimmung auf der Homepage abgebildet werden?

Hier spielen Urheberrecht und Datenschutz zusammen.
Bei anonymisierten Bildern muss grundsätzlich keine Zustimmung iSd EU-DSGVO eingeholt werden.

Fotos von urheberrechtlich geschützten Gebäuden, die beispielsweise von einem öffentlichen Ort aus angefertigt werden, unterliegen der Freiheit des Straßenbildes nach dem UrhG, sodass für eine Nutzung dieser Fotos keine Zustimmung eingeholt werden muss. Sind allerdings Daten auf diesen Bildern sichtbar, mit denen natürliche Personen identifiziert werden können oder identifizierbar sind, ist der Anwendungsbereich der EU-DSGVO gegeben. In einem solchen Fall müsste eine Einwilligung zur Verarbeitung gegeben sein.

Es wird diesbezüglich auch auf die Regelungen im 6. Abschnitt des Datenschutz-Anpassungsgesetz (DSAG 2018) verwiesen.

13. Stellt die Nutzung eines Firmenhandys mit Zugriff auf die Kunden-Kontaktdaten (Outlook-Adressen) und Nutzung diverser Apps (WhatsApp,…), welche auf die Handykontakte zugreifen, ein Problem im Sinne der EU-DSGVO dar? Gibt es dafür rechtliche (Zustimmungserklärung) oder technische (Einschränkung der Zugriffe nur auf Kontakte, die selbst solche Apps nutzen) Lösungen?

    Grundsätzlich muss die Zustimmung der Kunden zur Verarbeitung ihrer Daten eingeholt werden, soferne dies nicht zB zur Erfüllung einer vertraglichen Verpflichtung geschieht.

    Problematisch könnte zukünftig die Erstellung von internen Whats-App Gruppen sein, in denen Mitarbeiter personenbezogene Daten zu einem konkreten Projekt „verarbeiten". Da der Dienstgeber gegenüber eventuellen Datenschutzverletzungen seiner Mitararbeiter „Verantwortlicher" iSd EU-DSGVO ist, müsste er interne What's-App Gruppen, denen er selbst nicht beigetreten ist, verbieten, da er auf eventuelle Datenschutzverletzungen keinen Einfluss nehmen kann.

    Die Problematik ist allerdings allenfalls durch Einstellungen lösbar. Derartige Einstellungen sind aber oftmals nicht in der gewünschten Form vorhanden, sodass die DSGVO-konforme Anwendung einer bestimmten App unter Umständen nicht möglich sein kann.

14. Müssen sämtliche Projektunterlagen spätestens nach Ende der gesetzlichen Aufbewahrungspflichten (spätestens, unbewegliche Sache = 30 Jahre) gelöscht, entsorgt werden?

    Ähnlich siehe Frage 7 (Kapitel I).

    Grundsätzlich dürfen Daten iSd EU-DSGVO nicht länger als vereinbart oder unbedingt notwendig gespeichert oder verarbeitet werden. Auf Grund diverser gesetzlicher Verpflichtungen (Schadenersatz, Gewährleistung, Aufbewahrungsfristen, etc.) kann es allerdings notwendig sein, Daten über einen längeren Zeitraum aufzubehalten. Da allerdings auch die lange Nachhaftungsfrist nach 30 Jahren endet, müssen spätestens ab diesem Zeitpunkt sämtliche Daten gelöscht bzw. vernichtet werden (allenfalls anonymisiert).

15. Darf man Kontaktdaten von Kunden (Kundenkartei in Outlook) über die gesetzliche Aufbewahrungspflicht hinaus zum Zweck der Kundenbindung, Marketingmaßnahmen ohne gesonderte Zustimmung speichern ?

    Grundsätzlich nein. In solchen Fällen ist eine gesonderte Zustimmung der betroffenen Personen einzuholen.

16. Ab wann sind personenbezogene Daten ehemaliger Mitarbeiter spätestens zu löschen?

    Daten ehemaliger Mitarbeiter sind umgehend zu löschen, wenn sie nicht mehr benötigt werden (z.B. nach Ablauf von relevanten Fristen zur Aufbewahrung etc.).

    Sollen Daten länger gespeichert werden als unbedingt notwendig, oder länger als eine vertragliche oder gesetzliche Verpflichtung vorschreibt, müsste eine Zustimmung dafür eingeholt werden.

17. Wie sieht es mit bestehenden Kontaktdaten aus? Es geht hier um natürliche Personen. Wie sieht es mit Kontaktdaten von Firmenmitarbeitern aus, die notwendig sind, um Projekte abzuwickeln?

    Bereits bestehende Einwilligungen zur Datenverarbeitung bleiben auch weiterhin aufrecht, müssen allerdings innerhalb von 2 Jahren ab Inkraftreten der EU-DSGVO (also bis längstens 25.5.2020) auf das notwendige Niveau der Verordnung angepasst werden.

    Abermals ist anzumerken, dass Daten nur solange gespeichert werden dürfen, wie dies unbedingt erforderlich ist, ansonsten müsste ein Rechtmäßigkeitsgrund iSd Artikel 6 Abs. 1 EU-DSGVO vorliegen.

    Bei Firmenmitarbeitern, die notwendig sind, um Projekte abzuwickeln, wird es sich wieder um die Datenverarbeitung im Rahmen einer vertraglichen Verpflichtung handeln, sodass ein Rechtmäßigkeitsgrund zur Datenverarbeitung gegeben ist. Spätestens nach Projektabschluss müssen allerdings die Daten der Mitarbeiter gelöscht werden, sofern keine vertragliche oder gesetzliche Verpflichtung dieser Obliegenheit entgegensteht oder eine Einwilligung vorliegt.

18. Wie geht man mit dem E-Mail-Verkehr um? Muss alles verschlüsselt werden?

    Obsolet werden vermutlich E-Mails mit einer Vielzahl, darauf ersichtlichen, Empfängern sein. Im Sinne des Datenschutzes empfielt es sich, zukünftig vermehrt Adressaten lediglich unter Blind Carbon Copy (BCC) zu führen.

    Eine Verschlüsselung des gänzliche E-Mail Verkehrs erscheint zwar zweckdienlich, um das Risiko eines Data Breachs zu minimieren, die EU-DSGVO verlangt eine solche Maßnahme allerdings nicht. Es wird lediglich ein „angemessenen Sicherheitsniveau" gefordert, wobei dieser Begriff auf den konrekten Einfall anzuwenden und auszulegen ist. Konkrete Judikatur exisitert noch nicht.

19. Referenzen / Projektdatenblätter auf der Website - wie geht man in Zukunft damit um ?

    Sofern durch eine Veröffentlichung von Referenzen / Projektblättern auf einer Website personenbezogene Daten verarbeitet werden, muss die Zustimmung der Betroffenen eingeholt werden.

Ergänzend siehe Frage 12 (Kapitel I).

20. Was ist mit privaten Daten, die analog in den Akten vermerkt sind ?

In der EU-DSGVO wird nicht zwischen digitalen oder analogen Daten differenziert. Bei einer Verarbeitung von personenbezogenen Daten (digital oder analog), muss ein Rechtmäßigkeitsgrund iSd Artikel 6 Abs. 1 EU-DSGVO gegeben sein. Darüberhinaus sind solche Vorgänge in einem Verarbeitungsverzeichnis zu erfassen.

21. Grundsätzlich müssen ja Google und auch andere „Datensammler" z.B. bei Filmen (Streetview) Gesichter, Autokennzeichen usw. „verpixeln". Müssen auch Gebäudefassaden auf Wunsch des Eigentümers verpixelt werden? Wie schaut es mit Luftbildaufnahmen, besonders hinter dem Gebäude, Zaun usw. aus? Von der Straßenseite ist der Pool nicht erkennbar?

Hier handelt es sich vor allem um Fragen des Persönlichkeitsrechts und des Urheberrechts.

Aufnahmen dieser Art sind grundsätzlich nur mit Einwilligung der betroffenen Personen, sofern darauf sie selbst oder auch andere persönliche Dinge mit einem möglichen Rückschluss auf die betroffene Person zu sehen sind, zulässig. Ansonsten sind Daten wie Gesichter, Autokennzeichen etc. ohne Einwillung zu verpixeln. Auch Poolaufnahmen können höchstpersönliche Schutzbereiche darstellen, die ebenfalls zu verpixeln sind.

Lediglich Daten, die durch „Street View" verwendet werden, brauchen keine gesonderte Zustimmung, da diese unter die Panoramafreiheit bzw. unter die Freiheit des Straßenbildes nach dem Urheberrecht fallen.

Ergänzend siehe Frage 11 (Kapitel I).

Es wird diesbezüglich auch auf die Regelungen im 6. Abschnitt des Datenschutz-Anpassungsgesetz (DSAG 2018) verwiesen.

22. Durch den Einsatz div. Onlinedienste kann ich jetzt Daten natürlich schneller und im größeren Umfang abfragen. Kann es hier bei der Weiterverwendung zu Problemen kommen, vor allem, wenn ich quasi Massendaten mittels Computerprogramme über diverse Websites „absauge" ?

Wie sich das Ganze entwickelt, ist noch nicht abschließend abschätzbar. Auch das Land Steiermark mit seinen bereitgestellten Services (GIS) ist aktuell bei der Prüfung, ob diese Dienstleistungen weiterhin bestehen bleiben können.

Ergänzend siehe Frage 11 (Kapitel I).

Es wird diesbezüglich auch auf die Regelungen im 6. Abschnitt des Datenschutz-Anpassungsgesetz (DSAG 2018) verwiesen.

23. Welche Auswirkungen hat die EU-DSGVO auf einen Ziviltechniker, der eine Homepage betreibt? Welche technischen bzw. formalen Voraussetzungen müssen geschaffen werden, damit die Homepage den rechtlichen Ansprüchen der EU-DSGVO entspricht?

    - Anpassung der Datenschutzerklärung
    - Anpassung der Inhalte des Impressums
    - Entsprechener Passwortschutz, bzw. Schutzniveau bei den Zugängen zur Homepage, bzw. zum Serversystem, insbesondere bei Hompages mit Datenbanksystemen, welche personenbezogene Daten speichern

24. Wie muss man mit Wünschen umgehen, z.B. Rechnungen aus (alten) Buchhaltungen zu löschen? Wie kann man das machen, ohne die gesamte Buchhaltung zu vernichten? Darf man eine Buchhaltung auch länger als 7 Jahre aufbehalten?

    Grundsätzlich müssen Kollisionsnormen beachtet werden. Sollte es sich bei Unterlagen um "öffentliche" Urkunden handeln, so ist § 4 ZTG relevant. Danach sind einerseits elektronisch errichtete Urkunden und andererseits im Original beim Ziviltechniker verbleibende auf Papier errichtete öffentliche Urkunden für die Dauer von 30 Jahren aufzubewahren. Darüberhinausgehend sind diese Daten zu löschen.

    Dies trifft auch für die Daten der Buchhaltung zu. Da § 132 BAO eine 7 jährige Aufbewahrungsfrist und allenfalls darüber hinaus normiert, müssen diese Daten nach der gesetzlichen Aufbewahrungsfrist gelöscht werden, sofern sie nicht weiter benötigt werden. Aber trotzdem gilt das Gebot der Datenminimierung.

25. Frage bzgl. Plan einer Villa - der Bauherr wünscht vom Architekten die Löschung aller Daten nach Fertigstellung des Baus. Er möchte nicht, dass seine Pläne weiterhin beim ZT aufliegen.

    Sofern die Daten nicht weiter benötigt werden und der Auftraggeber die Löschung der personenbezogenen Daten fordert, ist diesem Wunsch nachzukommen.

    Ergänzend siehe Frage 10 (Kapitel I).

26. Muss ein ZT alle Kunden anschreiben, dass ihm erlaubt wird, elektronische Rechnungen zu legen? Reicht hier ein Passus im Vertrag? Ist das sowieso erlaubt/nicht erlaubt?

    Wiederum könnte sich die Rechtmäßigkeit der Verarbeitung aus der Erfüllung eines Vertrages ergeben, sodass für die Rechnungslegung an Kunden keine gesonderte Zustimmung erforderlich wäre. Grundsätzlich würde allerdings auch ein Vertragspassus sinnvoll sein.

II. Fragen zur Einwilligungserklärung

1. Gibt es für Architekten eine Mustervorlage für das Einholen der Zustimmungserklärung für die Verwendung der Daten lt. EU-DSGVO? (branchenübliche Verwendung personenbezogener Daten zur Auftragserfüllung, inkl. Weitergabe an alle Beteiligten zur Verwendung als Referenzen auf der Firmen-Homepage, zur Speicherung in einem Adressverzeichnis zum Versand von Newslettern)

   Entsprechende Muster sowie weitere Hilfestellungen finden Sie unter nachstehendem Link auf der Homepage der Bundeskammer der ZiviltechnikerInnen:

   https://www.arching.at/mitglieder/datenschutz/dsgvo_hilfestellungen.html

   Darüber hinaus wurde eine Datenschutz-Hotline für ZiviltechnikerInnen eingerichtet:
   Diese steht Ihnen im Mai und Juni 2018 von Mo-Fr (ausgenommen Feiertage) jeweils von 9 bis 14 Uhr unter der Nummer 0800-180081 zur Verfügung.

2. Wie muss eine Einwilligungserklärung zur Datenverarbeitung aussehen und wann muss eine solche eingeholt werden ?

   Datenverarbeitungen sind nur rechtmäßig, wenn mindestens eine der Bedingungen iSd Artikel 6 erfüllt ist, also ein Vertrag, eine rechtliche Grundlage oder die Zustimmung des Betroffenen.

III. Fragen zum Datenverarbeitungsregister/Risikobewertung

1. Pflicht zur Führung eines „Verzeichnisses von Verarbeitungstätigkeiten": Sind hier Verarbeitungen, wie Verwendungen der personenbezogenen Daten (Name, Anschrift/Kontaktdaten) im Zuge der Auftragserfüllung, Projektbearbeitung (z.B.: Planung Wohnhaus: Verwendung der Daten auf Plänen, Beschreibungen & Baubesprechungsprotokollen,…) betroffen und ist somit jede Versendung z.B.:Aussendung von Informationen an alle Betroffenen (Miteigentümer, Anrainer, ausführende Firmen, beteiligte Fachplaner, Behörden,…) zu erfassen?

   Grundsätzlich sind jegliche Vorgänge in einem Verarbeitungsverzeichnis zu erfassen, wenn personenbezogene Daten verarbeitet werden. In den obigen Fällen müsste daher eine solche Verarbeitungen dokumentiert werden.

2. Würde eine solche Verarbeitung (siehe Frage 1 [Kapitel III]) die Ausnahmeregelungen für Unternehmen unter 250 Mitarbeiter erfüllen?

   Die Ausnahmeregelung für Unternehmer unter 250 Mitarbeiter iSd Artikel 30 Abs. 5 ist nur anzuwenden, sofern die von den Unternehmen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich

erfolgt und nicht die Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt.

Ziviltechniker werden vermutlich meist nicht unter diese Ausnahmeregelung fallen.

IV. Fragen zum Datenschutzbeauftragten

1. Wie wirkt sich die Verordnung generell auf eine Vermessungskanzlei aus?

   Siehe Frage 2 (Kapitel IV).

2. Was muss ein Ziviltechniker formal beachten bzw. umsetzen, um nicht nach der EU-DSGVO „bestraft" zu werden?

   - Erfassung der Datenverarbeitungen in einem Verarbeitungsverzeichnis
   - Überarbeitung von Datenschutzerklärungen
   - Anpassung von Verträgen
   - Eventuelle Bestellung eines Datenschutzbeauftragen
   - Anpassung der Impressumsbestimmungen
   - Abschluss von Geheimhaltungserklärungen
   - Einholung von Zustimmungserklärungen
   - Angemessenes Schutzniveau bei den verwendeten IT Systemen

   Ergänzend siehe Frage 1 (Kapitel VII).

V. Fragen zu technisch-/organisatorischen Maßnahmen

1. Was ist zum Datenschutzbeauftragten zu sagen? Notwendig?

   - Grundlegendes zum DSB:

   Ein DSB ist auf jeden Fall zu benennen, wenn

   a) die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeiten handeln,

   b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder

   c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten

gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.

- Mögliche Interpretation von obiger Formulierung:

Wenn die Kerntätigkeit mit der Datenverarbeitung in einem untrennbaren Zusammenhang steht, muss auch die Datenverarbeitung der Kerntätigkeit zugeordnet werden, was im **Zweifel** die Benennung eines DSB zur Folge haben könnte.

Beispiel Gesundheitsvorsorge: Zwar ist die Hauptaufgabe eines Krankenhauses die Gesundheitsvorsorge der Patienten. Da eine solche Vorsorge allerdings ohne die Verarbeitung von personenbezogenen Patientendaten nicht aufrecht erhalten werden kann, ist die eigentliche Kerntätigkeit mit der Datenverarbeitung untrennbar verbunden, sodass auch in solchen Fällen im Zweifel ein DSB zu bestellen wäre.

- Herrschende Meinung:

Nach herrschender Meinung ist ein DSB nur für jene Unternehmen vorgeschrieben, deren **Kerntätigkeit** (=HAUPTTÄTIGKEIT) zur umfangreichen, regelmäßigen und systematischen Überwachung von betroffenen Personen führt oder die **umfangreich** sensible Daten – nunmehr: besondere Kategorien von Daten – oder Daten über Strafdaten umfasst. Umfangreich ist nach Interpretation der „Artikel-29-Datenschutzgruppe", die die EU-Kommission berät, etwa die Verarbeitung von Gesundheitsdaten in einem Krankenhaus, nicht jedoch durch einen einzelnen Arzt.

Im großen Graubereich dazwischen muss zwar nicht, sollte aber dennoch sinnvollerweise ein DSB bestellt werde. Das gilt allerdings nicht für jedes kleinere oder mittlere Unternehmen (KMU), zumal bei der Mehrzahl dieser Unternehmen die Kerntätigkeit keine umfangreiche Verarbeitung umfasst.

- Ist ein DSB bei einem durchschnittlichen ZT-Büro zu bestellen?

Im Zweifel sollte man daher bei einem normalen ZT-Büro eher von einer restriktiven Wortinterpretation des Artikel 37 ausgehen.

Da die Kerntätigkeit eines Architekturbüros, Vermessungsbüros etc. nicht die Verarbeitung von personenbezogenen Daten, sondern vorrangig Planungs- oder Vermessungsaufgaben sind, muss in der Regel kein DSB bestellt werden. Hier liegt noch ein großer Bereich der Unsicherheit vor.

2. Besteht für ein klassisches Architekturbüro die Verpflichtung der Bestellung eines Datenschutzbeauftragten? Welche Fälle von Verarbeitungen könnten zu einer solchen Verpflichtung führen, betrifft das z.B. das Führen einer Kundenkartei (zB.: Outlook-Kontaktdaten) zum Verschicken von Newslettern oder Einladungen/Informationen zu wiederkehrenden Veranstaltungen ?

Siehe Frage 1 und 2 (Kapitel III).

VI. Fragen betreffend Anträgen von Personen (zB Auskunft, Abändern, Löschen)

1. Welche Daten konkret sind hier im Falle einer Anfrage bekanntzugeben? Nur Kontaktdaten, die in einer Datenbank oder einem Verzeichnis geführt werden? Oder auch Briefe und Emails (wie auf der WKO-Seite angegeben)? Wenn ja, welche Kriterien muss ein Email/Brief erfüllen, damit er der Auskunftspflicht unterliegt? Sind Informationen & Pläne zu privaten Liegenschaften (Lagepläne, Bestandspläne & Einreichpläne), Auszüge aus Grundstücksdatenbanken usw. ebenfalls zu übermitteln ? Wer trägt die Kosten für eine solche umfangreiche Herausgabe der „Daten", Projektunterlagen? Kann man dafür Aufwandsentschädigungen verlangen, sollten diese im Anbot oder Auftrag bereits angegeben werden?

   Es sind alle konkreten personenbezogenen Daten bekannt zugeben. Bei Briefen und Emails ist auf das Briefgeheimnis, insbesondere bezüglich Dritter zu achten, welches bei der Bekanntgabe von Emails/Briefen unter Umständen verletzt sein könnte. Informationen und Pläne zu privaten Liegenschaften (Lagepläne, Bestandspläne & Einreichpläne), Auszüge aus Grundstücksdatenbanken sind zu prüfen, ob personenbezogene Daten enthalten sind. Sollten personenbezogene Daten vorhanden sein, sind diese ebenfalls zu übermitteln oder die personenbezogene Daten zu anonymisieren, schwärzen, bzw. zu löschen. Die Kosten für die einmalige Herausgabe trägt der Datenverarbeiter, eine Aufwandsentschädigung ist für eine Kopie der Daten in der DSGVO nicht vorgesehen.

VII. Gesonderte Fragen aus dem Publikum

1. Was muss ein durchschnittliches ZT-Büro bei der Umsetzung der EU-DSVGO grundlegend beachten?

   - Dokumentation der internen Datenverarbeitungen („Verarbeitungsregister")
   - Schulungsverpflichtungen gegenüber den Mitarbeitern (Verschwiegenheitsverpflichtung, Auskunftserteilungen, Recht im Umgang mit Daten etc.)
   - Aufklärungs-, Warnpflichten gegenüber den Kunden
   - Beachtung von Kollisionsnormen (Urheberrecht, Persönlichkeitsrecht, § 132 BAO etc.)
   - Generelle Reduktion von Datenspeicherungen
   - Anpassung der internen EDV-Systeme (zB Firewall, W-Lan Zugänge, Netzwerksicherheit, Passwörter, etc.)
   - Verschlüsselung von Notebooks und externen Datenträgern
   - Anpassung der Bürostrukturen (Alarmsystem, Versperren der Aktenschränke etc.)
   - Backups einrichten

- Verpflichtungen für Mitarbeiter schriftlich festhalten

2. Gelten Veröffentlichungen von Kontaktdaten der Mitarbeiter auf Internetseiten (beispielsweise KAGES) als Zustimmung zur Verarbeitung (ablegen, abspeichern) dieser Daten?

   Nein. Eine solche Serviceleistung bietet lediglich die Möglichkeit zur leichteren Kontaktaufnahme. Daraus kann allerdings keine generelle Einwilligung der Mitarbeiter abgeleitet werden, dass ihre Daten verarbeitet werden.

3. Muss von jeder Person, die auf einer Projektbeteiligungsliste aufscheint, eine Zustimmung zur Datenerhebung eingefordert werden?

   Soweit die Verarbeitung zur Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen, muss keine Zustimmung eingeholt werden.

   Bei der Datenverarbeitung von Personen, die in keinem Zusammenhang mit einer vertraglichen Verpflichtung stehen und wenn auch keine sonstigen Rechtfertigungsgründe iSd Art. 6 Abs. 1 EU-DSGVO vorliegen, ist eine gesonderte Einwilligung erforderlich.

4. Welche Qualifikationen muss ein Datenschutzbeauftragter (DSB) erfüllen? Ist ein Diplom erforderlich?

   Die EU-DSGVO definiert kein detailliertes Anforderungsprofil.

   In Aritkel 37 Abs. 5 EU-DSGVO wird lediglich festgelegt, dass der Datenschutzbeauftragte auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt wird, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben. Weiters darf kein Interessenskollision bestehen.

   Es ist kein Diplom bzw. keine Zertifizierung erforderlich.

   Näheres dazu findet sich in den Leitlinien in Bezug auf Datenschutzbeauftragte („DSB") von der „ARTIKEL-29-DATENSCHUTZGRUPPE" (https://www.dsb.gv.at/documents/22758/112500/Leitlinien_in_Bezug_auf_Datenschutzbeauftragte.pdf/d241f0fd-6908-44fd-a12a-0f861e7a1dfb)

5. Welche Stellung nimmt ein DSB im Betrieb ein?

   Grundsätzlich wird ein DSB eine Stellung zwischen den Dienstnehmern und Dienstgebern, ähnlich eines Betriebsrates, einnehmen, ohne den selben Kündigungsschutz zu genießen. Er wird den Dienstgeber beraten, gegebenfalls „zurechtweisen" und auch kontrollieren müssen.

Es können sowohl interne als auch externe Mitarbeiter zum DSB bestellt werden. Bei einem internen Mitarbeiter ist allerdings die Haftung von Relevanz, da man bei einem Data Breach unter das DHG fallen würde (Reduktion beim Regress). Ein externer DSB hingegen würde bei einem Verstoß voll haften.

6. Wer ist der „Verantwortliche" bei einer GmbH iSd EU-DSGVO?

   Primär die GmbH selbst, allerdings können auch die Geschäftsführer (Geschäftsführerhaftung) heranzgezogen werden.

7. Muss, und wenn ja bis wann, ein Datenschutzbeauftragter namhaft gemacht werden?

   Betreffend den Voraussetzungen für die Bestellung eines Datenschutzbeauftragten wird auf die Beantwortung der Frage 45 verwiesen.

   Sind die Voraussetzungen für die Bestellung eines Datenschutzbeauftragten erfüllt, muss dieser der Aufsichtsbehörde mitgeteilt werden. Dies hat bis zum Inkrafttreten der EU-DSGVO (25.5.2018) zu erfolgen.

8. Muss auch ein EPU einen DSB bestellen?

   Wenn die Voraussetzungen für die Bestellung eines DSB gegeben sind, ja!

   Bei einem durchschnittlichen Ziviltechnikerbüro werden in der Regel die Voraussetzungen für die Bestellung eines DSB nicht vorliegen.

   Näheres siehe Frage 1 und 2 (Kapitel IV).

9. Genügt für die Rechtmäßigkeit der Datenverarbeitung, dass man einen Vertragspassus in sein Angebot aufnimmt, indem man darauf hinweist, dass bei einer Auftragserteilung Daten verarbeitet werden?

   Ja. Grundsätzlich sind solche Klauseln auch in AGBs denkbar, wenn sie nicht „versteckt" platziert werden und für einen durchschnittlichen Verbraucher erkennbar sind. Die Sprache muss einfach, lesbar und verständlich sein.

10. Dürfen Bewerbungsunterlagen verspeichert werden?

    Auch hier besteht die grundsätzliche Löschungsverpflichtung, wenn die Daten nicht mehr benötigt werden. Alternativ könnte man den Bewerber um seine Einwilligung ersuchen, dass seine Bewerbungsunterlagen in Evidenz gehalten werden, solange dem nicht widersprochen wird.

11. Darf man ohne Zustimmung Fotos von seinen Mitarbeitern veröffentlichen?

Nein, außer es wurde ein entsprechender Passus der Genehmigung in den jeweiligen Arbeitsverträgen aufgenommen (Persönlichkeitsrecht – Recht am eigenen Bild).

12. Welche Hinweise müssen bei den Impressumsbestimmungen auf der Homepage aufgenommen werden (DSB, etc.)?

    Hinweise finden Sie auf der Website der Bundeskammer für ZiviltechnikerInnen.

    Den dazugehörigen Link finden Sie bei Frage 1 (Kapitel II).

13. Muss allen Geschäftspartnern eine Zustimmungserklärung übermittelt werden, damit diese Daten auch weiterhin „legal" verwendet werden dürfen? Darf diese Zustimmungserklärung auch digital, also per Email, übermittelt werden ?

    Bereits bestehende Zustimmungserklärungen bleiben auch weiterhin aufrecht, müssen allerdings binnen 2 Jahren ab Inkraftreten der EU-DSGVO an die Bestimmungen der Verordnung angepasst werden.

    Die Zustimmungserklärung ist an keine bestimmte Form gebunden, muss aber nachweislich sein.

    Zur Erfüllung eines Vertragsverhältnis wäre die Verarbeitung von personenbezogenen Daten ohnehin rechtmäßig iSd EU-DSGVO.

    Ergänzend siehe Frage 17 (Kapitel I).

14. Wenn ein Mitglied Visitenkarten von Besprechungen, Konferenzen etc. erhält, müssen auch diese Personen ihre Zustimmungserklärungen abgeben, damit diese Visitenkarten abgelegt werden dürfen ?

    Ist die Datenverarbeitung für die Erfüllung eines Vertrages notwendig, brauchen Sie keine Zustimmung Ihrer Vertragspartner einholen. Sollten allerdings Visitenkarten von vertraglich unabhängigen Personen abgelegt bzw. nach Vertragsbeendigung archiviert werden, müssten Sie eine Zustimmung einfordern.

    Nach Vertragsabschluss sind sämtliche Visitenkarten zu vernichten oder es muss eine nachträgliche Zustimmung eingeholt werden.

15. Soll die Ablage (Verwaltung der Daten) in Hardcopy erfolgen, oder darf sie auch digital sein – Stichwort Verarbeitungsverzeichnis?

    Die Ablage kann sowohl digital als auch analog erfolgen.

    Ergänzend siehe Frage 1 (Kapitel III).

16. Müssen alle Mitarbeiter eine Geheimhaltungserklärung unterzeichnen?

Es empfiehlt sich, sämtliche Mitarbeiter sowie auch Reinigungs(Putz)dienste und dergleichen eine Geheimhaltungserklärung unterzeichnen zu lassen. Bei neuen Mitarbeitern könnte eine solche Vereinbarung in den Dienstverträgen aufgenommen werden. Ist in einem Betrieb ein Betriebsrat eingerichtet, könnte auch eine Betriebsvereinbarung abgeschlossen werden.

Hinzuweisen ist allerdings abermals darauf, dass bereits bestehende Geheimhaltungserklärungen auch mit Inkrafttreten der Verordnung weiterhin aufrecht bleiben, lediglich an die formalen Voraussetzungen der Verordnung binnen 2 Jahren anzupassen sind.

17. Was wird unter dem Begriff „Standardanwendung" verstanden ?

Unter einer Standardanwendung werden Programme wie bspw. Microsoft Office (Word, Exel, Access etc.) verstanden. Es handelt sich dabei also um Software, die für einen breiten Bereich überlicherweise zB in Unternehmen anfallender Standardtätigkeiten verwendet wird.

18. Was ist eine „Datenschutz-Folgenabschätzung" ?

Siehe Frage 11 (Kapitel I).

RA Dr. Rainer BECK, MMag.art.

Dipl.-Ing. Dr.techn. Peter Anton MANDL