II

Sanktionen bei Verstößen

Wie in jedem anderen Lebensbereich ist auch bei der Umsetzung der datenschutzrechtlichen Vorgaben die Frage nach dem „Warum“ ein wesentlicher Grundbaustein, um in die Umsetzung zu kommen. Denn Architekten/Ingenieure haben mit ihrem Alltagsgeschäft genug zu tun, sodass jede Zusatzaufgabe, die unnötig Ressourcen in Anspruch nimmt, zu vermeiden ist. Die Beachtung der datenschutzrechtlichen Vorgaben sollte jedoch nicht zu den zu vermeidenden Aufgaben gehören.

Denn bei Missachtung von und Verstößen gegen die datenschutzrechtlichen Vorgaben sehen diese, anders als vor der Geltung der DSGVO, nunmehr erhebliche Sanktionen vor. Neben dem Reputationsschaden, den Architekten/Ingenieure bei Kunden bzw. in der öffentlichen Wahrnehmung erleiden können, können die mit der DSGVO eingeführten neuen und drastisch erhöhten Geldbußen Architekten/Ingenieuren erheblich schaden.

Der Bußgeldrahmen geht nach den Bestimmungen der DSGVO nunmehr bis hin zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes, je nachdem, was höher ist. Die Höhe des Bußgelds wird von den zuständigen Aufsichtsbehörden im jeweiligen Einzelfall verhängt und hängt u.a. maßgeblich von Art und Umfang des Verstoßes ab.

Neben den drastischen Bußgeldern können folgende Sanktionen auf Architekten/Ingenieure zukommen, sollten sie die datenschutzrechtlichen Vorgaben missachten oder gegen diese verstoßen:

- Die zuständigen Aufsichtsbehörden können grundsätzlich (unangekündigte) Prüfungen durchführen und hierbei auch den Zugang zu den Geschäftsräumen einschließlich aller Datenverarbeitungsanlagen/-geräte fordern.
- Die zuständigen Aufsichtsbehörden sind gemäß den Bestimmungen der DSGVO u.a. auch dazu berechtigt, vom datenschutzrechtlich Verantwortlichen (z.B. dem Inhaber des Planungsbüros) die Zurverfügungstellung aller Angaben und Informationen zu verlangen, die die Aufsichtsbehörde für die Erfüllung ihrer Aufgaben (Überwachung und Durchsetzung der DSGVO) benötigt.
- Die zuständigen Aufsichtsbehörden sind gemäß Art. 58 DSGVO dazu berechtigt, all diejenigen Abhilfemaßnahmen vorzunehmen, durch die sie einen Verantwortlichen oder Auftragsverarbeiter warnen können, dass ein beabsichtigter Verarbeitungsvorgang aller Wahrscheinlichkeit nach gegen die DSGVO verstoßen wird.
- Die zuständigen Aufsichtsbehörden dürfen im Einzelfall nach ihrem Ermessen einen Verantwortlichen oder Auftragsverarbeiter auch verwarnen, wenn er gegen die DSGVO verstoßen hat (Merke: Ein Bußgeld ist bei Verstößen nicht zwingend!).

Die Grundvoraussetzung für die Anwendung der DSGVO ist, dass personenbezogene Daten verarbeitet werden. Ist dies nicht der Fall, sind auch die Bestimmungen der DSGVO nicht zu beachten. Was heißt das genau? Was sind personenbezogene Daten und was nicht? Wann können Architekten/Ingenieure die DSGVO außen vor lassen?

1. Was sind personenbezogene Daten?

Der Begriff der „personenbezogenen Daten“ wird in Art. 4 Nr. 1 DSGVO vom Gesetzgeber legaldefiniert als

„Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“.

Vom Datenschutz nach der DSGVO werden also zunächst sämtliche Informationen und Angaben erfasst, die sich unmittelbar oder mittelbar auf eine natürliche Person, d.h. auf einen Menschen beziehen. Diese Definition ist in der Praxis äußerst weit auszulegen. Personenbezogene Daten bzw. Einzelangaben mit Personenbezug sind beispielsweise:

- Name und sonstige Identifikationsmerkmale (z.B. Geburtsdatum, Namenszusätze, Ausweisnummer)
- Kontaktdaten (z.B. Postanschrift, E-Mail-Adresse, Telefonnummer)
- körperliche/physische Merkmale (z.B. Größe, Gewicht, Haarfarbe, genetischer Fingerabdruck, Krankheiten, Drogenkonsum)
- geistige Zustände/psychische Merkmale (z.B. Wünsche, Einstellungen, Überzeugungen, Geschäftsfähigkeit)
- Verbindungen und Beziehungen (z.B. Verwandtschafts- und Freundschaftsverbindungen, Arbeitgeber)
- sonstige Informationen, die auf eine natürliche Person Rückschlüsse zulassen (z.B. Standortdaten, Nutzungsdaten, Handlungen, Äußerungen, Werturteile, beruflicher Werdegang, Bankverbindungen)

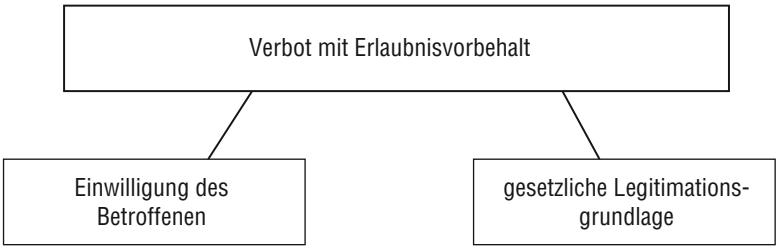
1.1 Natürliche Person – juristische Person

Ein wesentliches Abgrenzungsmerkmal ist der Personenbezug der jeweiligen Daten. Personenbezogen sind Daten nur dann, wenn sie sich auf eine „natürliche Person“ im Rechtssinn beziehen. Das heißt, es wird jeder lebende Mensch unabhängig vom Alter und der Nationalität und auch unabhängig von der Geschäftsfähigkeit von der DSGVO erfasst.

nung des Anwendungsbereichs der DSGVO), ob für die Datenverarbeitung eine Legitimationsgrundlage existiert.

Die Legitimationsgrundlage benötigen Architekten/Ingenieure auch für die Dokumentation im Verarbeitungsverzeichnis (siehe im Folgenden).

Der Grundsatz des Verbots mit Erlaubnisvorbehalt kann bildlich vereinfacht wie folgt dargestellt werden:



Die DSGVO gibt den Verantwortlichen die Erlaubnistatbestände in Art. 6 DSGVO vom Grundsatz her vor. Demnach dürfen Architekten/Ingenieure als Verantwortliche Daten u.a. dann verarbeiten, wenn

a) eine (wirksame) **Einwilligung** des Betroffenen vorliegt,
b) die **Verarbeitung zur Erfüllung des Vertrags** dient (z.B. Abwicklung eines Vertrags),
c) die Verarbeitung der **Durchführung von vorvertraglichen Maßnahmen dient**, die auf Anfrage der betroffenen Person erfolgen (z.B. Übersendung von Prospekten/Angeboten),
d) die Verarbeitung der **Erfüllung rechtlicher Pflichten** dient,
e) eine **Interessenabwägung** die Verarbeitung zugunsten des Architekten/Ingenieurs legitimiert (z.B. Werbemaßnahmen ohne Einwilligung).

3.2 Exkurs: Werbung und Verarbeitung personenbezogener Daten

Die bisherigen Regelungen im BDSG zur Werbung wurden vollständig durch die DSGVO abgelöst. Das bisherige sogenannte Listenprivileg oder eine Privilegierung von Daten aus öffentlichen Verzeichnissen oder Quellen kennt die DSGVO nicht. Noch nicht geklärt ist, inwieweit die geplante neue E-Privacy-Verordnung im Bereich der elektronischen Werbung konkrete Regelungen für Werbung enthalten wird.

Seit Geltung der DSGVO muss der Verantwortliche im Falle einer (bloßen) Verletzung des Schutzes personenbezogener Daten dies *unverzüglich* und *möglichst binnen 72 Stunden*, nachdem ihm die Verletzung bekannt wurde, der zuständigen Aufsichtsbehörde melden, Art. 33 Abs. 1 DSGVO.

Die Meldepflicht entfällt nur dann, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Hier haben die Verantwortlichen einen Abwägungs- und Entscheidungsspielraum, wobei dieser Spielraum nicht zu weit ausgereizt und die Abwägung in jedem Fall dokumentiert werden sollte. Denn kommt es zu einer Kontrolle durch die zuständigen Aufsichtsbehörden, greift auch hier wieder die Umkehr der Beweislast. Das heißt, der Verantwortliche muss nachweisen, dass und warum eine Meldung der Datenpanne nach seiner Auffassung nicht erforderlich war. Im Zweifel sollten sich die Verantwortlichen hier fachkundigen Rat einholen.

Kommt der Verantwortliche zu dem Ergebnis, dass die Datenpanne der zuständigen Aufsichtsbehörde gemeldet werden muss, muss – neben der Frist – auch der Mindestinhalt beachtet werden. Die Meldung an die **Aufsichtsbehörde** muss nach den Vorgaben der DSGVO nämlich folgende Mindestangaben beinhalten:

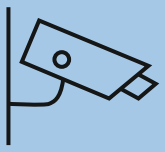
Mindestangaben zur Meldung an Aufsichtsbehörden nach DSGVO

Mindestangaben zur Meldung einer Datenpanne an die Aufsichtsbehörde nach DSGVO	Enthalten
Beschreibung der Art der Verletzung des Schutzes der personenbezogenen Daten und, soweit möglich, dies auch mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen	
Beschreibung der Datenkategorien und der ungefähren Zahl der betroffenen Datensätze	
Nennung der Namen und der Kontaktdaten des Datenschutzbeauftragten (sofern vorhanden) oder einer sonstigen Anlaufstelle für weitere Informationen	
Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten	
Beschreibung der ergriffenen und vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und	
ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen	

Folgendes Symbolbild hat sich etabliert:

Beispiel für ein Hinweisschild gemäß Art. 13 DSGVO

Achtung Videoüberwachung



Name + Kontaktdaten des Verantwortlichen:

Name + Kontaktdaten des Datenschutzbeauftragten (sofern vorhanden):

Zweck + Rechtsgrundlage der Datenverarbeitung (und ggf. berechtigte Interessen):

Speicherdauer/Berechnung:

Weitere Informationen sind unter www.mustermann.de/datenschutz zu finden.

5. Auskunftspflichten vs. Auskunftsrechte

Eine weitere Pflicht des Verantwortlichen und spiegelbildlich ein besonderes Recht von Betroffenen ist das Auskunftsrecht. Das Auskunftsrecht wird in Art. 15 DSGVO und für bestimmte Fälle ergänzend in §§ 29, 24 BDSG gesetzlich geregelt.

Macht der Betroffene sein Recht auf Auskunft geltend, kann er gemäß Art. 15 DSGVO grundsätzlich folgende Informationen vom Verantwortlichen verlangen:

1. die Verarbeitungszwecke
2. die Kategorien personenbezogener Daten, die verarbeitet werden
3. die Empfänger oder Kategorien von Empfängern, denen die Daten offengelegt wurden
4. falls möglich, die Dauer der Speicherung bzw. die Kriterien für die Festlegung/Berechnung der Dauer
5. die Rechte des Betroffenen
6. das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
7. wenn die personenbezogenen Daten *nicht* bei der betroffenen Person erhoben wurden, alle verfügbaren Informationen über die Herkunft der Daten
8. das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling