8 HINWEISE ZUM UMGANG MIT DER DATENSCHUTZ-GRUNDVERORDNUNG DS-GVO (MIT MUSTERN)[1]

*Die Datenschutz-Grundverordnung (DS-GVO) kommt nach einer Übergangsfrist ab dem **25. Mai 2018** zur Anwendung und gilt in der ganzen EU unmittelbar für Behörden und Unternehmen. Gleichzeitig tritt ein neues Bundesdatenschutzgesetz in Kraft, das den Datenschutz nicht mehr vollständig regelt, sondern nur noch die Ausnahmeregelungen enthält, welche die DS-GVO zulässt (z.B. zum Beschäftigten-Datenschutz). Auch das Landesdatenschutzgesetz NRW wird überarbeitet. Dieses richtet sich aber nicht an Architekturbüros, sondern bspw. an die Architektenkammer NRW.*

HINWEIS 1:
Zur Erfüllung eines Architektenvertrages ist eine Datenverarbeitung ohne Einwilligung weiterhin zulässig. Auch im vorvertraglichen Bereich ist keine Einwilligung notwendig (z.B. Verarbeitung der E-Mail-Adresse des Bauherrn, um ihm einen Kostenvorschlag zu zusenden).

HINWEIS 2:
Werden Daten eines Bauherrn verarbeitet, so soll dieser darüber informiert werden, welche Daten erhoben und zu welchem Zweck sie genutzt werden. Ein **MUSTER 1** über die Information liegt anbei; das Muster betrifft den Fall, dass Daten direkt vom Architekten erhoben und verarbeitet werden.

HINWEIS 3:
Ein Datenschutzbeauftragter wird in einem Architekturbüro grundsätzlich erst dann notwendig, wenn es mindestens 10 Personen angestellt hat, die sich ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.

HINWEIS 4:
Architekturbüros müssen sämtliche Verarbeitungsprozesse in einem „Verzeichnis von Verarbeitungstätigkeiten“ dokumentieren. Erweist sich eine beabsichtigte Datennutzung als risikoreich, ist eine „Datenschutz-Folgenabschätzung“ vorzunehmen. Ein **MUSTER 2** für ein Verarbeitungsverzeichnis ist beigefügt.

HINWEIS 5:
Personen, deren Daten verarbeitet werden, haben ein besonderes Auskunftsrecht. Mit diesem Auskunftsrecht können sie erfahren, ob über sie personenbezogene Daten gespeichert oder verarbeitet werden. Sofern solche Daten vom Architekturbüro gespeichert werden, muss das Büro Auskunft über die Daten, die Herkunft sowie die Informationen erteilen. Ein **MUSTER 3** zur Beantwortung einer Auskunftsanfrage liegt anbei.

HINWEIS 6:
Da Architekten personenbezogene Daten von Bauherrn in der Regel speichern, besteht die Pflicht, diese Daten mit technischen und organisatorischen Maßnahmen zu schützen. Es gilt dabei der Grundsatz, je mehr und je sensibler die Daten sind, die verarbeiten werden, desto mehr Schutz ist notwendig. Ein **MUSTER 4** stellt einen Maßnahmenkatalog vor.

HINWEIS 7:
Bauherrn und andere Personen, deren Daten Architekten speichern, stehen besondere Lösch- und Sperrrechte zu. Wenn eine Verarbeitung unrechtmäßig oder nicht mehr notwendig ist, wenn Widerspruch gegen die Verarbeitung eingelegt wurde, besteht eine Handlungspflicht. Wichtig ist, dass vorzeitig (ggf. mit dem IT-Anbieter) untersucht und geprüft wird, wie Daten vollständig und dauerhaft gesperrt und gelöscht werden können.

[1] Diese Hinweise und Muster wurden von der Architektenkammer Baden-Württemberg erstellt und der Architektenkammer NRW freundlicherweise zur Verfügung gestellt.

Hinweis 8:
Bitte beachten Sie auch den Praxishinweis Nr. 54 der Architektenkammer NRW „EU Datenschutz-Grundverordnung“. Dort wird ein Überblick über die grundlegenden Neuregelungen des Datenschutzrechts im Zuge der Umsetzung der DS-GVO gegeben.

Hinweis der AKNW: Dieses Merkblatt kann nur eine Erstinformation darstellen und eine individuelle Beratung im Einzelfall nicht ersetzen. Die Muster sind Orientierungshilfen. Jedes Architekturbüro muss sich individuell mit den Anforderungen des Datenschutzrechts auseinandersetzten und dafür möglicherweise auch externe Unterstützung – etwa durch Rechtsanwaltskanzleien etc. – in Anspruch nehmen.

MUSTER 1

Informationen zur Datenerhebung gemäß Artikel 13 DS-GVO

Mustermann Architekten GmbH, Hauptstraße 1, 40000 Düsseldorf

erhebt Ihre Daten zum Zweck der Vertragsdurchführung, zur Erfüllung ihrer vertraglichen und vorvertraglichen Pflichten sowie zur Direktwerbung.

Die Datenerhebung und Datenverarbeitung ist für die Durchführung des Vertrags erforderlich und beruht auf Art. 6 Abs. 1 lit. a und b DS-GVO. Eine Weitergabe der Daten an Dritte findet nicht statt. Die Daten werden gelöscht, sobald sie für den Zweck ihrer Verarbeitung nicht mehr erforderlich sind.

Sie haben das Recht, der Verwendung Ihrer Daten zum Zweck der Direktwerbung jederzeit zu widersprechen. Zudem sind Sie berechtigt, Auskunft der bei uns über Sie gespeicherten Daten zu beantragen sowie bei Unrichtigkeit der Daten die Berichtigung oder bei unzulässiger Datenspeicherung die Löschung der Daten zu fordern. Sie können uns erreichen unter

Architekturbüro Monika Mustermann
Hauptstraße 1
40000 Düsseldorf
Telefon: (0211) 123 456
Telefax: (0211) 123 789
E-Mail: post@mustermann.de

Ihnen steht des Weiteren ein Beschwerderecht bei der Aufsichtsbehörde zu. Die Aufsichtsbehörde ist

Die Landesbeauftragte für Datenschutz und
Informationsfreiheit Nordrhein-Westfalen
Postfach 20 04 44
40102 Düsseldorf
Tel.: 0211/38424-0
Fax: 0211/38424-10
E-Mail: poststelle@ldi.nrw.de

MUSTER 2/a

Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen

Angaben zum Verantwortlichen

1. Verantwortlich

Mustermann Architekten GmbH, Hauptstraße 1, 40000 Düsseldorf

2. Gesetzlicher Vertreter (= Geschäftsführung / Betriebsinhaber)

Frau Monika Mustermann, Hauptstraße 1, 40000 Düsseldorf

3. Zuständige Aufsichtsbehörde

Die Landesbeauftragte für Datenschutz und
Informationsfreiheit
Nordrhein-Westfalen
Postfach 20 04 44
40102 Düsseldorf
Tel.: 0211/38424-0
Fax: 0211/38424-10
E-Mail: poststelle@ldi.nrw.de

4. Regelungen zur Datensicherheit

Sicherheitskonzept vom. 1. Januar 2018 von IT-Mayer Schulze
(Königstraße 2, 70000 Stuttgart)

5. Sachverhalte zu Drittstaatenübermittlungen

Eine Drittstaatenübermittlung gibt es nicht

MUSTER 2/b

Verzeichnis von Verarbeitungstätigkeiten

Verzeichnis Nr. 1

☐ Ersterstellung
☐ Änderung eines bestehenden Verzeichnisses

Erstellungsdatum: TT.MM.JJJJ

Bezeichnung der Verarbeitungstätigkeit:

Erstellung und Führung der Kundendatei

I. Angaben zur Verantwortlichkeit

1. Verantwortlicher Fachbereich/verantwortliche Führungskraft

Sonja Mustermann

2. Bei gemeinsamer Verantwortlichkeit:

Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen

II. Angaben zur Verarbeitungstätigkeit

3. Risikobewertung / Besteht bei der Verarbeitung ein hohes Risiko für die betroffenen Personen?

☐ Nein
☐ Ja

Wenn ja, dann Durchführung einer Datenschutz-Folgenabschätzung erforderlich (Art. 35 DS-GVO). Datenschutz-Folgenabschätzung als separate Anlage beifügen.

4. **Zwecke der Verarbeitungen/der Verarbeitungstätigkeit**

Organisation von Geschäftskontakten und Bestandskunden.

Durchführung von Architektenverträgen

5. Rechtsgrundlage der Verarbeitungen/der Verarbeitungstätigkeit

Art. 6 Abs. 1 lit. b DS-GVO

6. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, Art. 30 Abs. 1 S. 2 lit. c DS-GVO

6.1. Betroffene Personengruppen	**6.2. Kategorien personenbezogener Daten**
Bauherr	Name, Vorname, Adressdaten, (elektronische) Kontaktdaten ggfs. Firma, Datum des Auftrags, Gegenstand des Auftrags

7. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden

7.1. Interne Empfänger	Mitarbeiter: Herrn Ernst Mustermann
7.2. Externe Empfänger	Nein
7.3. Vertragliche Dienstleister (Vertrag der Auftragsdatenverarbeitung als Anlage beifügen)	Nein

8. Datenübermittlungen in Drittländer oder an internationale Organisationen, Art. 30 Abs. 1 S. 2 lit. e DS-GVO

- ☐ Nein
- ☐ Ja

Wenn ja, dann: Name des Drittlandes / der internationalen Organisation (DS-GVO)

9. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien, Art. 30 Abs. 1 S. 2 lit. f DS-GVO

Die Daten werden gelöscht, wenn sie für die Erfüllung des Zweck (siehe Nr. 4) nicht mehr erforderlich sind.

10. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 S. 2 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO

Siehe betriebsinternes IT-Sicherheitskonzept

10.1 Art der eingesetzten DV-Anlagen und Software (optional)

Siehe betriebsinternes IT-Sicherheitskonzept

10.2 Konkrete Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 S. 2 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO

Siehe betriebsinternes IT-Sicherheitskonzept

MUSTER 3/a

Auskunft eines Architekten an Bauherrn

Frau
Tine Test
Rathausplatz 1
40000 Düsseldorf

Sehr geehrte Frau Test,

mit Schreiben vom 1. Juni 2018 baten Sie uns um Auskunft, welche Daten wir zu Ihrer Person gespeichert haben. Sie sind bei uns in der Kundendatei als Bauherrin erfasst.

Zur Datenverarbeitung durch unser Unternehmen teilen wir Ihnen mit, dass die Datenerhebung zur Kommunikation mit Ihnen, Abgabe von Angeboten, Abrechnung von Leistungen oder zur Erfüllung von Verträgen erfolgt. Diese Daten haben Sie uns mitgeteilt. Der Gesetzgeber hat vielfältige Aufbewahrungspflichten und -fristen erlassen. Nach Ablauf dieser Fristen werden die entsprechenden Daten routinemäßig gelöscht, sofern sie nicht mehr zur Vertragserfüllung erforderlich sind. Sofern Daten hiervon nicht erfasst sind, werden sie gelöscht, sobald sie für den Zweck, für den sie erhoben wurden, nicht mehr benötigt werden. Die Daten werden nicht an Dritte weitergeben. Die über Sie gespeicherten Daten entnehmen Sie bitte der beigefügten Tabelle.

Sofern die aufgeführten Daten nicht (mehr) richtig sind, wären wir Ihnen über eine entsprechende Korrektur und Rückmeldung dankbar.

Sie haben das Recht, sich bei der für uns zuständigen Datenschutzaufsichtsbehörde zu beschweren

Die Landesbeauftragte für Datenschutz und
Informationsfreiheit Nordrhein-Westfalen
Postfach 20 04 44
40102 Düsseldorf
Tel.: 0211/38424-0
Fax: 0211/38424-10
E-Mail: poststelle@ldi.nrw.de

falls Sie der Meinung sind, dass die Verarbeitung Ihrer personenbezogenen Daten nicht rechtmäßig erfolgt.

Gerne stehen wir Ihnen für weitere Fragen oder Auskünfte zur Verfügung

Mit freundlichen Grüßen

Anlage

MUSTER 3/b

DATENBLATT FÜR BAUHERRN

Familienname:	Bauer
Vorname:	Bernadette
Geburtsname:	Beate
Geschlecht:	weiblich
Geburtsdatum:	1. Januar 1970
Staatsangehörigkeit:	deutsch
Titel:	Dr. iur.
Straße:	Marktplatz 1
PLZ:	70000
Wohnort:	Stuttgart
Ust.-ID.:	123 456 789
Festnetz:	0711 123 457
Mobil:	0121 123 456
Telefax:	0711 123 890
E-Mail:	bbb@bauer.de
Bankname:	Bauerbank
IBAN-Nummer:	DE 11 123 4456 789
BIC:	

Weitere individuelle Daten

MUSTER 4

Technische und organisatorische Maßnahmen

Folgende technische und organisatorische Maßnahmen wurden getroffen:

A. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen mit denen personenbezogene Daten verarbeitet werden, zu verwehren

1. Technische Maßnahmen

- ☐ Alarmanlage
- ☐ Türsicherung (elektrischer Türöffner, Zahlenschloss usw.)
- ☐ Schlüsselregelung (Schlüsselverwaltung: Schlüsselausgabe etc.)
- ☐ Sicherheitsschlösser
- ☐ _____

2. Organisatorische Maßnahmen

- ☐ Protokollierung der Besucher / Besucherbuch
- ☐ Schlüsselregelung / Schlüsselbuch
- ☐ Videoüberwachung der Zugänge
- ☐ _____

B. Zugangskontrolle

Maßnahme, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können

1. Technische Maßnahmen

- ☐ Authentifikation mit Benutzer + Passwort
- ☐ Aktuelle Anti-Viren-Software
- ☐ Aktuelle Firewall
- ☐ VPN-Technologie
- ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form bzw. Verschlüsselung
- ☐ E-Mail-Verschlüsselung
- ☐ Verschlüsselung von Datenträgern
- ☐ _____

2. Organisatorische Maßnahmen

- ☐ Zuordnung und Verwaltung der Benutzerberechtigungen
- ☐ Erstellen von Benutzerprofilen
- ☐ Passwortvergabe / Passwortregeln (inkl. regelmäßigen Änderungen)
- ☐ Automatische Sperrung des Arbeitsplatzes
- ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☐ Protokollierung von Übermittlungen

☐ Erstellung einer Übersicht von Datenträgern, Aus- und Eingang
☐ _____

C. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass Personen nur im Rahmen ihrer Zugriffsberechtigung auf Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können

1. Technische Maßnahmen

☐ Einsatz von Aktenvernichter
☐ Einsatz von Datenträgervernichter
☐ Einsatz von Dienstleistern unter Beachtung von DIN 66399
☐ Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
☐ Verschlüsselung von Datenträgern
☐ Verschlüsselung von Smartphones
☐ _____

2. Organisatorische Maßnahmen

☐ Verwaltung der Benutzerrechte durch System-Administrator
☐ Anzahl der Administratoren auf das "Notwendigste" reduziert
☐ Erstellung eines Berechtigungsplans
☐ Passwortrichtlinie inkl. Länge und Wechsel
☐ Sichere Aufbewahrung von Datenträgern
☐ Ordnungsgemäße Vernichtung von Datenträgern
☐ Löschungskonzept für Daten
☐ Protokollierung der Vernichtung von Daten
☐ Protokollieren von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
☐ _____

D. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist

1. Technische Maßnahmen

☐ Einrichtungen von VPN-Tunneln
☐ E-Mail-Verschlüsselung
☐ _____

2. Organisatorische Maßnahmen

☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten

Überlassung bzw. vereinbarter Löschfristen

☐ Erstellung einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgänge

☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

☐ _____

E. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

1. Technische Maßnahmen:

☐ Protokollierung der Eingabe, Änderung und Löschung von Daten

☐ _____

2. Organisatorische Maßnahmen:

☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden

☐ Protokollauswertungsroutinen/-systeme vorhanden

☐ Aufbewahrungs-/Löschungsfrist für Protokolle vorhanden

☐ _____

F. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können

1. Technische Maßnahmen:

☐ _____

2. Organisatorische Maßnahmen:

☐ Vorhandene Vereinbarungen zur Auftragsverarbeitung

☐ Kontrolle der Vertragsausführung

☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

☐ _____

G. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind

1. Technische Maßnahmen:

☐ Unterbrechungsfreie Stromversorgung (USV)

☐ Überspannungsschutz

☐ Schutz gegen Umwelteinflüsse (Sturm, Wasser)

☐ Feuer- und Rauchmeldeanlagen

- ☐ Feuerlöscher in Serverraum
- ☐ Klimaanlage in Serverraum
- ☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverraum
- ☐ Schutzsteckdosen in Serverraum
- ☐ _____

2. Organisatorische Maßnahmen:

- ☐ Erstellen eines Notfallplans
- ☐ Alarmmeldung bei unberechtigten Zutritten zu Serverraum
- ☐ Testen von Datenwiederherstellung
- ☐ Serverraum nicht unter sanitären Anlagen
- ☐ Serverraum über Wassergrenze (in Hochwassergebiet)
- ☐ Erstellen eines Backup- (Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und -ort) und Recoverykonzepts
- ☐ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☐ Spiegelung von Festplatten (z. B. RAID-Verfahren)
- ☐ _____

H. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können

1. Technische Maßnahmen:

- ☐ Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☐ Bei pseudonymisierten Daten: Trennung der Zuordnungsdaten und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- ☐ _____

2. Organisatorische Maßnahmen:

- ☐ Festlegung Technologie von Datenbankrechten
- ☐ Festlegung von Datenbankrechten
- ☐ Erstellung eines Berechtigungskonzepts
- ☐ _____

I. Dokumentationskontrolle

Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können

1. Technische Maßnahmen:

- ☐ Zulässigkeit eines Datentransfers in Drittländer ist gegeben
- ☐ _____

2. Organisatorische Maßnahmen

- ☐ Führung eines Verarbeitungsverzeichnisses

☐ Dokumentation der eingesetzten IT- Systeme und deren Systemkonfiguration
☐ _____

J. Allgemeine Maßnahmen

☐ Ist ein betrieblicher Datenschutzbeauftragter bestellt?
☐ Nein
☐ Ja
Name: _____
Funktion: _____
E-Mail: _____
Telefon: _____

☐ Mitarbeiter wurden über Datenschutzrecht und Datensicherheit geschult.
Am: _____/ Vom: _____

☐ Alle Mitarbeiter sind auf das Datengeheimnis, ggf. auf das Fernmeldegeheimnis, verpflichtet.

☐ Es existieren verfahrensunabhängige Plausibilitäts- und Sicherheitsprüfungen (z.B. technisch unterstützt oder durch Externe).

☐ Ein Datensicherheitskonzept / Informationssicherheitsmanagement ist vorhanden.

☐ Ein Datenschutzkonzept ist vorhanden.

☐ Eine Auditierung/Zertifizierung ist vorhanden (Prüfung der Einhaltung am _____ _____und Bestätigung s. Anlage _____).

☐ Verhaltensregeln nach Art. 40 DSGVO sind vorhanden (Unterwerfung am _____ _____und Bestätigung s. Anlage _____).