ZDH
ZENTRALVERBAND DES
DEUTSCHEN HANDWERKS

Leitfaden

Das neue Datenschutzrecht

Was öffentlich-rechtliche Handwerkorganisationen zu beachten haben

Gültig ab 25. Mai 2018

Abteilung Organisation und Recht

DAS HANDWERK
DIE WIRTSCHAFTSMACHT. VON NEBENAN.

Vorwort

Ab 25. Mai 2018 gelten in allen Mitgliedstaaten der Europäischen Union neue Datenschutzregeln. Mit der Reform soll sichergestellt werden, dass in allen Mitgliedstaaten derselbe Datenschutzstandard besteht. Da in Deutschland bereits hohe Anforderungen an den Datenschutz gelten, führen die neuen Vorschriften zwar zu zahlreichen formellen Änderungen. Eine inhaltliche Verschärfung der Anforderungen geht mit der Reform jedoch insgesamt nicht einher.

Handwerksorganisationen müssen sicherstellen, dass sie bis zum 25. Mai 2018 die erforderlichen Anpassungen vornehmen. Der vorliegende Leitfaden thematisiert die für die Praxis wichtigsten Aspekte und Fragen. Er bietet neben rechtlichen Erklärungen zahlreiche Beispielsfälle, Checklisten und Muster, die in der Praxis genutzt werden können.

Der Leitfaden zielt darauf ab, öffentlich-rechtlichen Handwerksorganisationen einen vertieften Überblick sowie das notwendige Rüstzeug zu geben, die jeweiligen organisationsinternen Abläufe an die Anforderungen des neuen Datenschutzrechts anzupassen. Eine rechtlich abschließende und verbindliche Beratung kann der Leitfaden nicht leisten. Auf Handwerksorganisationen, die nicht öffentlich-rechtlich, sondern privatrechtlich konstituiert sind, ist dieser Leitfaden nicht anwendbar. Für privatrechtliche Handwerksorganisationen gelten die Ausführungen des Leitfadens für Handwerksbetriebe entsprechend.

Inhaltsverzeichnis

Seite

1. Zulässige Datenverarbeitung ohne Einwilligung

Wann ist die Nutzung von Daten erlaubt?

Eine Datennutzung ist nur zulässig, wenn

- eine gesetzliche Vorschrift sie erlaubt oder
- derjenige, dessen Daten verarbeitet werden sollen, in die Nutzung von Daten einwilligt (siehe Kapitel 2 „Anforderungen der datenschutzrechtlichen Einwilligung“, S. 6).

Gesetzliche Erlaubnis

Vorschriften, die eine Datennutzung erlauben, finden sich hauptsächlich in Artikel 6 der Europäischen Datenschutz-Grundverordnung (DSGVO). Diese Regelungen werden durch die Landesdatenschutzgesetze ergänzt. Zudem finden sich für öffentlich-rechtliche Stellen des Handwerks insbesondere in der Handwerksordnung gesetzliche Ermächtigungen zur Datenverarbeitung.

Art. 6 DSGVO

Gemäß Art. 6 DSGVO ist eine Datenverarbeitung ohne Einwilligung insbesondere in zwei, für öffentliche Stellen relevanten, Fällen zulässig.

- **Art. 6 Abs. 1 c) DSGVO**
  Die Datenverarbeitung ist zulässig, wenn sie zur **Erfüllung einer rechtlichen Verpflichtung** erforderlich ist. Hier sind die konkreten Ermächtigungen zur Verarbeitung von Daten nach der HwO zu beachten (§§ 5a, 6, 8 Abs. 3 S. 2, 13 Abs. 5, 17 Abs. 2, 19, 28, 54 Abs. 1, 87, 91 Abs. 1, 113 Abs. 2, 118a HwO). Siehe zur Führung der Handwerksrolle und des Verzeichnisses zulassungsfreier Handwerke und handwerksähnlicher Gewerbe Kapitel 9 „Rechtskonforme Verwendung von Daten aus der Handwerksrolle“ (S. 26) sowie zur Lehrlingsrolle Kapitel 10 „Rechtssicherer Umgang mit Daten aus der Lehrlingsrolle“ (S. 29).

- **Art. 6 Abs. 1 e) DSGVO**
  Die Datenverarbeitung ist zulässig, wenn sie **für die Wahrnehmung einer Aufgabe** erforderlich ist, die **im öffentlichen Interesse** liegt oder in Ausübung **öffentlicher Gewalt** erfolgt (z.B. Soll- und Kann-Aufgaben der Innungen nach § 54 Abs. 2, 3 HwO und der Handwerkskammern gemäß § 91 Abs. 2, 3 HwO).

Beachte: Wird die Datenverarbeitung auf diese Rechtsgrundlage gestützt, haben betroffene Personen gemäß Art. 21 DSGVO jederzeit ein Widerrufsrecht. Widerspricht der Betroffene, darf die Datenverarbeitung dennoch fortgeführt werden, wenn ein zwingendes öffentliches Interesse an der Verarbeitung besteht, das den Interessen des Betroffenen überwiegt.

Regelungen der Landesdatenschutzgesetze

Die Anpassung der Landesdatenschutzgesetze an die DSGVO ist zum Stand November 2017 noch in keinem Bundesland erfolgt. Es ist absehbar, dass die Landesdatenschutzgesetze wie bisher Regelungen zur Datenverarbeitung durch öffentliche Stelle enthalten werden.

Nach § 3 BDSG ist die Verarbeitung personenbezogener Daten durch öffentliche Stellen zulässig, wenn sie zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgabe erforderlich ist. Hierdurch wird Art. 6 DSGVO konkretisiert, ohne dass damit eine inhaltliche Einschränkung verbunden ist.

2. Anforderungen der datenschutzrechtlichen Einwilligung

Einwilligung

Eine Datennutzung ist nur zulässig, wenn

- eine gesetzliche Vorschrift sie erlaubt oder
- derjenige, dessen Daten verarbeitet werden sollen, in die Datennutzung einwilligt.

Eine rechtmäßige Datennutzung setzt deshalb entweder eine gesetzliche Erlaubnis (siehe hierzu Kapitel 1 „Zulässige Datenverarbeitung ohne Einwilligung“, S. 4) oder eine Einwilligung des Betroffenen voraus.

Damit eine Einwilligung wirksam ist, müssen die gesetzlichen Anforderungen an eine Einwilligungserklärung erfüllt sein. Für öffentlich-rechtliche Handwerksorganisationen gelten die Vorschriften der Europäischen Datenschutzgrundverordnung (Artikel 7 DSGVO), die durch die jeweiligen Landesdatenschutzgesetze ergänzt werden.

Einwilligungen müssen freiwillig sein

Eine Einwilligung ist nur rechtmäßig, wenn derjenige, der die Einwilligung erklärt, dies freiwillig tut. Jede Form von Druck, Zwang oder Verpflichtung führt deshalb zur Unwirksamkeit der Einwilligung. Die DSGVO geht auch dann von einer Unfreiwilligkeit aus, wenn zwischen der einwilligenden Personen und dem Datenverarbeiter ein „klares Ungleichgewicht besteht“ (Erwägungsgrund 43 DSGVO). Ein solches Ungleichgewicht unterstellt die DSGVO grundsätzlich, wenn es sich bei dem Datenverarbeiter um eine Behörde handelt. Behörden, die Daten auf Grundlage einer Einwilligung verarbeiten, müssen deshalb künftig darlegen und beweisen können, dass kein Ungleichgewicht besteht und die Einwilligung freiwillig erfolgt. Die Darlegung wird Handwerksorganisationen jedoch allein deshalb gelingen, weil Einwilligungen – wenn überhaupt – nur außerhalb des gesetzlichen und hoheitlichen Tätigkeitsbereichs der Handwerksorganisationen in Frage kommen, und dort keine klassische „Behörden-Bürger-Beziehung“, sondern ein Mitgliedschaftsverhältnis zwischen Handwerksbetrieben und Handwerksorganisation besteht.

Besonderheiten bei Minderjährigen

Die Wirksamkeit einer Einwilligung ist nicht vom Alter des Einwilligenden abhängig. Insofern spielt es an sich keine Rolle, ob es sich um einen Minderjährigen oder einen Volljährigen handelt. Eine Sonderreglung besteht lediglich für Telemedienangebote. Hier ist eine Einwilligung von Personen unter 16 Jahren unwirksam (Art. 8 DSGVO).

Abgesehen von Telemedien kommt es für die Wirksamkeit der Einwilligung allein auf die Einsichtsfähigkeit des Einwilligenden in die Tragweite seiner Erklärung an. Ob Minderjährige diese Einsichtsfähigkeit besitzen, kann nicht pauschal beurteilt werden, sondern richtet sich nach den Umständen des Einzelfalls. Da die Einsichtsfähigkeit eines Minderjährigen nicht in jedem Fall mit abschließender Sicherheit beurteilt werden kann, empfiehlt es sich in der Praxis, bei Minderjährigen stets die Einwilligungserklärung der Erziehungsberechtigten einzuholen.

Textform

Einwilligungen müssen – anders als früher – nicht mehr schriftlich erklärt werden. Eine mündliche Einwilligung ist deshalb in gleicher Weise wirksam. Allerdings sollte die Einwilligungserklärung allein aus Beweis- und Dokumentationsgründen stets in Textform eingeholt werden.

Die Form der Einwilligung ist zugleich Maßstab für den Fall, dass die Einwilligung nachträglich widerrufen wird. Wurde die Einwilligung mündlich erteilt, ist ein mündlich erklärter Widerruf zu akzeptieren. Die Dokumentation mündlicher Erklärungen ist jedoch aufwändig, fehleranfällig und für effiziente Abläufe nicht zu empfehlen.

Welchen Inhalt müssen Einwilligungserklärungen haben?

Die gesetzlichen Vorschriften geben klare Mindestanforderungen an Einwilligungen vor.

- Der Datenverarbeiter muss seine Identität offenlegen (Angabe des Namens der Handwerksorganisation).
- Es muss dargelegt werden, welche Daten erhoben werden (z.B. Adressdaten, Kontodaten).
- Es muss der Zweck genannt werden, für den die Daten verarbeitet werden (z.B. Werbung).
- Hinweis auf das Widerrufsrecht: Der Einwilligende hat die Einwilligung freiwillig erklärt und kann sie jederzeit mit Wirkung für die Zukunft widerrufen. Es ist anzugeben, in welcher Form (Textform) und an welche Adresse (Postanschrift, E-Mail-Adresse) der Widerruf zu richten ist.

Die Angaben müssen verständlich und in klarer, einfacher Sprache formuliert werden. Sie müssen so konkret und so umfassend sein, dass sich der Einwilligende darüber ein Bild machen kann, was mit seinen Daten passiert.

Optische Gestaltung

Die Einwilligungserklärung ist so zu gestalten, dass sie vom Einwilligenden wahrgenommen wird. Dies ist vor allem dann wichtig, wenn die Einwilligungserklärung zusammen mit anderen Informationen (z.B. Allgemeinen Geschäftsbedingungen) in einem einzigen Text vorgelegt wird. Eine optische Abhebung ist z.B. durch Einrahmung, Fettdruck, eine andere Farbe oder Schriftgröße möglich.

Aktive Erklärung erforderlich

Die Einwilligung muss aktiv und durch eine eindeutige Handlung erklärt werden. Dies kann – abgesehen von einer unterschriebenen Einwilligung – z.B. durch Anklicken eines Kästchens auf einer Internetseite geschehen. Stillschweigen oder das bloße Hinnehmen bereits angekreuzter Kästchen stellen keine Einwilligung dar.

Soll die datenschutzrechtliche Einwilligung gemeinsam mit weiteren Erklärungen abgegeben werden, so sollte für jede Erklärung eine gesonderte Unterzeichnung oder ein gesondertes Anklicken vorgesehen werden. Dies bietet sich allein aus Beweiszwecken an. Eine einzige Unterschrift/Bestätigung für das gesamte Dokument birgt dagegen das Risiko der Unzulässigkeit und ist deshalb nicht zu empfehlen.

Wie lange gilt eine Einwilligung?

Obwohl die gesetzlichen Vorschriften keine zeitliche Geltungsdauer vorsehen, gehen Rechtsprechung und Aufsichtsbehörden davon aus, dass erklärte Einwilligungen nicht unbeschränkt gültig sind. Eine Einwilligung kann nur herangezogen werden, solange derjenige, der eingewilligt hat, vernünftiger Weise mit einer Verarbeitung seiner Daten rechnen muss. Dies kann je nach Fall unterschiedlich lang sein. Wer seine Einwilligung zum Erhalt von Einladungen zu Informationsveranstaltungen erklärt hat, muss nicht damit rechnen, dass er nach mehreren Jahren erstmals oder erneut eine Einladung erhält. Anders verhält es sich bei Einwilligungen zum Erhalt von Einladungen zu Sommerfesten, die nur jährlich stattfinden.

<u>Weiterführende Unterlagen:</u>

Anlage 1: Muster einer Einwilligungserklärung

3. Formelle Pflichten – Ein Überblick

Welchen Zweck verfolgen die Pflichten?

Das Datenschutzrecht räumt Personen, deren Daten von öffentlich-rechtlichen Stellen genutzt werden, umfassende Rechte ein. Mithilfe dieser Rechte soll erreicht werden, dass die Betroffenen Einfluss auf den Umgang und die Verbreitung ihrer Daten haben.

Für Handwerksorganisationen, die Daten verarbeiten, bestehen kehrseitig zum Teil hohe Anforderungen an die Datennutzung. Wer Daten z.B. seiner Mitglieder nutzen möchte, muss diese überwiegend formalen Anforderungen erfüllen. Die Pflichten von Handwerksorganisationen und die Rechte von Betroffenen sind in den Artikeln 12 bis 22 der Datenschutz-Grundverordnung (DSGVO) geregelt. Die Vorschriften werden an verschiedener Stelle durch die Landesdatenschutzgesetze ergänzt.

Transparenzgebot (Art. 12 DSGVO)

Art. 12 regelt den Umgang mit Anfragen des Betroffenen und in welcher Form Anfragen zu beantworten sind. Der Verantwortliche hat der betroffenen Person sämtliche Informationen und alle Mitteilungen auf präzise, transparente, verständliche und leicht zugängliche Weise in einer klaren und einfachen Sprache unverzüglich zu übermitteln. Obwohl auch eine mündliche Information zulässig ist, ist in der Praxis die Textform allein aus Beweisgründen zu empfehlen. Hierbei spielt es keine Rolle, ob der Text in Papierform oder elektronisch übermittelt wird.

Informationspflichten (Art. 13 und 14 DSGVO)

Art. 13 regelt, welche Informationen der Verantwortliche dem Betroffenen zu erteilen hat, wenn er beim Betroffenen Daten erhebt. Art. 14 bestimmt die Informationspflichten, wenn die Daten nicht bei der betroffenen Person selbst, sondern bei einem Dritten erhoben werden. Siehe hierzu ausführlich Kapitel 4 „Informationspflichten bei Erhebung personenbezogener Daten“, S. 12).

Auskunftsrecht (Art. 15 DSGVO)

Betroffene haben das Recht, von der datenverarbeitenden Stelle eine Bestätigung zu verlangen, ob über sie personenbezogene Daten gespeichert sind und verarbeitet werden. Ist das der Fall, hat die öffentliche Stelle Auskunft über diese Daten, deren Herkunft sowie weitere Informationen zu erteilen. In der Praxis werden solche Auskunftsanfragen i.d.R. von Mitglie-

dern auf Handwerksorganisationen zukommen (siehe hierzu Kapitel 5 „Erteilung von Auskünften, S. 15).

Recht auf Berichtigung (Art. 16 DSGVO)

Sind personenbezogene Daten falsch, nicht mehr aktuell oder unvollständig, haben die betroffenen Personen gemäß Art. 16 ein Recht auf Berichtigung. Der verantwortliche Datenverarbeiter muss die unrichtigen oder unvollständigen Daten unverzüglich korrigieren.

Recht auf Löschung (Art. 17 DSGVO)

Nach Art. 17 haben Betroffene das Recht, die Löschung ihrer Daten zu verlangen, wenn einer der gesetzlich geregelten Löschungsgründe vorliegt. Ein solcher Grund liegt vor, wenn:

- die Aufbewahrung der Daten für den Zweck, zu dem sie ursprünglich erhoben wurden, nicht mehr erforderlich ist,
- die Daten unrechtmäßig verarbeitet wurden,
- der Betroffene seine Einwilligung für eine weitere Speicherung widerrufen hat.

Selbst wenn einer dieser Gründe vorliegt, dürfen Daten nicht gelöscht werden, wenn gesetzliche Aufbewahrungsfristen bestehen und der Verantwortliche zur Aufbewahrung verpflichtet ist (z.B. rentenrelevante Unterlagen von Mitarbeitern).

Anstelle der Löschung tritt die „Einschränkung der Verarbeitung“, wenn die Löschung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist und das Löschungsinteresse des Betroffenen als gering anzusehen ist (siehe hierzu unten).

Recht auf Vergessenwerden (Art. 17 DSGVO)

Eine besondere Form des Löschungsanspruchs ist das „Recht auf Vergessenwerden“. Dieses Recht bezieht sich auf Daten, die veröffentlicht wurden und zielt insbesondere auf Veröffentlichungen im Internet ab.

Die betroffene Person muss den Datenverarbeiter darüber informieren, dass sie die Löschung aller Daten, einschließlich sämtlicher Kopien und Links zu diesen Daten verlangt. Der Verantwortliche muss neben der Löschung zusätzlich alle Personen, die mit den jeweiligen Daten arbeiten, darüber informieren, dass die Daten zu löschen sind. Zu denken ist hier an erster Stelle an Suchmaschinen, die ebenfalls über den Löschungsantrag informiert werden müssen.

Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)

Mit dem Recht auf Einschränkung der Verarbeitung können Betroffene erwirken, dass der Datenverarbeiter ihre Daten sperrt und nicht weiter verarbeiten darf. Dies gilt u.a. für den Fall, dass

- die Richtigkeit der Daten bestritten wird und die Datennutzung für die Dauer der Überprüfung der Richtigkeit ausgesetzt werden soll,
- die Datenverarbeitung unrechtmäßig ist und der Betroffene anstatt der Löschung die Nutzungseinschränkung bevorzugt.

Datenübertragung (Art. 20 DSGVO)

Betroffene haben den Anspruch, eine Kopie der sie betreffenden personenbezogenen Daten in einem üblichen Dateiformat zu erhalten. Der Betroffene soll damit Daten von einem Anbieter zu einem anderen „mitnehmen“ können. Die Regelung zielt insbesondere auf einen leichteren Wechsel bei sozialen Netzwerken und Verträgen mit Energieversorgern und Banken. Das Recht ist jedoch auf Daten beschränkt, die der Betroffene dem Verantwortlichen freiwillig zur Verfügung gestellt hat. Für Handwerksorganisationen hat dieses Recht keine nennenswerte Praxisrelevanz.

Widerspruchsrecht (Art. 21 DSGVO)

Betroffenen steht ein Widerspruchsrecht gegen eine Datenverarbeitung zu, wenn die Verarbeitung zur Erfüllung einer Aufgabe erfolgt, die im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erfolgt (siehe hierzu Kapitel 1 „Datenverarbeitung ohne Einwilligung“, S. 4). Nach erfolgtem Widerspruch dürfen die Daten nicht mehr zur Direktwerbung genutzt werden.

Dokumentationspflicht (Art. 30 DSGVO)

Handwerksorganisationen sind verpflichtet, sämtliche Verarbeitungsprozesse im sog. „Verzeichnis von Verarbeitungstätigkeiten“ zu dokumentieren. Zudem ist bei risikoreichen Datennutzungen zusätzlich eine „Datenschutz-Folgenabschätzung“ nach Art. 35 DSGVO vorzunehmen. Siehe hierzu ausführlich Kapitel 6 „Dokumentationspflicht“, S. 18.

4. Informationspflichten bei Erhebung personenbezogener Daten

Transparenz durch Informationen

Personen, deren Daten von einem anderen verarbeitet werden, sollen im Vorlauf zur Datenverarbeitung umfassend informiert werden. Insbesondere sollen sie erfahren, welche Daten über sie erhoben und zu welchem Zweck sie genutzt werden. Um diese Transparenz herzustellen, sind Handwerksorganisationen verpflichtet, den jeweils betroffenen Personen zahlreiche Informationen über die beabsichtigte Datennutzung zu erteilen. Welche Informationen dies im Einzelnen sind, ist in den Art. 13 und 14 der Europäischen Datenschutz-Grundverordnung (DSGVO) aufgelistet, die durch die entsprechenden Vorschriften der jeweiligen Landesgesetzes ergänzt werden.

Bei den Informationspflichten sind drei Situationen zu unterscheiden:

- Die Daten werden bei der Person, deren Daten verarbeitet werden sollen, direkt erhoben.

- Die Daten, die verarbeitet werden sollen, werden nicht bei der betroffenen Person selbst, sondern von einem Dritten erhoben.

- Der Datenverarbeiter hat die Daten bereits vorliegen und möchte die Daten zu einem anderen Zweck nutzen, als zu dem, zu dem sie ursprünglich bei der betroffenen Person erhoben wurden.

Erhebung personenbezogener Daten beim Betroffenen selbst (Art. 13 DSGVO)

Werden personenbezogene Daten beim Betroffenen direkt erhoben, müssen diesem insbesondere folgende Informationen mitgeteilt werden:

- **Identität des Verantwortlichen**: Name und Kontaktdaten des Datenverarbeiters, Name des Vertreters (z.B. Name des Präsidenten und Hauptgeschäftsführers).

- **Kontaktdaten des Datenschutzbeauftragten (DSB):** Der Name des DSB muss hierbei nicht genannt werden (siehe Kapitel 7 „Der Datenschutzbeauftragte“, S. 21).

- **Verarbeitungszweck der Datennutzung**: Z.B. zur Erfüllung der gesetzlichen Aufgaben.

- **Rechtsgrundlage der Datenverarbeitung:** Entweder Benennung der gesetzlichen Norm, die die Datenerhebung erlaubt (siehe hierzu Kapitel 1 „Datenverarbeitung ohne Einwilligung“, S. 4) oder Einwilligung des Betroffenen (siehe hierzu Kapitel 2 „Anfor-

derungen der datenschutzrechtlichen Einwilligung“, S. 6). Bei einer Einwilligung ist zusätzlich der Hinweis auf das **Recht zum Widerruf der Einwilligung** erforderlich.

- **Empfänger** oder Kategorien von Empfängern der Daten: Gilt nur, wenn die Daten an Dritte weitergeleitet werden (z.B. Weitergabe von Daten an andere öffentliche Stellen).

- **Dauer der Verarbeitung** oder Dauer der Datenspeicherung: In der Regel dauert die Datennutzung an, bis der Zweck der Datenverarbeitung erreicht ist.

- **Rechte der Betroffenen**: Z.B. Recht auf Auskunft, Berichtigung, Löschung (siehe hierzu Kapitel 3 „Formelle Pflichten – Ein Überblick“, S. 9).

- Hinweis auf das **Beschwerderecht bei der Aufsichtsbehörde.**

- Hinweis, ob die **Bereitstellung der Daten gesetzlich vorgeschrieben ist**: Z.B. Angaben zur Eintragung in die Handwerksrolle gemäß § 6 Abs. 1 HwO in Verbindung mit Anlage D zur HwO.

Erhebung personenbezogener Daten bei Dritten (Art. 14 DSGVO)

Werden personenbezogene Daten nicht beim Betroffen selbst, sondern bei einem Dritten oder aus öffentlichen Quellen erhoben, müssen zunächst dieselben Angaben gemacht werden, wie bei der Erhebung beim Betroffenen selbst.

Zusätzlich sind dem Betroffenen zwei weitere Informationen zu erteilen:

- Welche **Kategorien** personenbezogener Daten erhoben werden: Werden z.B. einfache Adressdaten oder besonders sensible Daten wie z.B. Gesundheitsdaten erhoben?

- Aus welcher **Quelle** die personenbezogenen Daten stammen und ob es sich dabei um eine öffentlich zugängliche Quelle handelt.

Zweckänderung

Für den Fall, dass der Verantwortliche die Daten bereits vorliegen hat und für einen anderen Zweck weiterverarbeiten möchte, muss er die betroffenen Personen vor der Weiterverarbeitung über folgende Aspekte informieren:

- den neuen Zweck der Verarbeitung,

- die Dauer der Verarbeitung (siehe oben Erhebung beim Betroffenen),
- die Rechte des Betroffenen (siehe oben Erhebung beim Betroffenen),
- Beschwerderecht (siehe oben Erhebung beim Betroffenen).

Wann ist zu informieren?

Im Fall der Datenerhebung beim Betroffenen müssen die Informationen im Zeitpunkt der Datenerhebung mitgeteilt werden. Werden die Daten nicht beim Betroffenen erhoben, muss der Verantwortliche die Informationen innerhalb einer angemessenen Frist, spätestens jedoch nach einem Monat erteilen. Bei einer Zweckänderung ist der Betroffene vor der Verwendung der Daten zum neuen Zweck zu unterrichten.

Gibt es Ausnahmen von der Informationspflicht?

Die Information des Betroffenen ist nicht erforderlich, soweit dieser bereits Kenntnis über die einzelnen Angaben der Datenverarbeitung hat.

Werden die Daten bei einem Dritten erhoben, darf die Information zudem unterbleiben, wenn die Informationserteilung unmöglich ist oder einen unverhältnismäßigen Aufwand erfordern würde.

Sind Formvorschriften zu beachten?

Die Informationen müssen nach Maßgabe von Art. 12 Abs. 1 DSGVO in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache erteilt werden (siehe hierzu **Anlage 2**).

Die Übermittlung der Informationen sollte grundsätzlich in Textform erfolgen. Obwohl auch eine mündliche Information möglich ist, sollte in der Praxis allein aus Beweisgründen die Textform gewählt werden. Hierbei spielt es keine Rolle, ob der Text in Papierform oder elektronisch übermittelt wird.

5. Die Erteilung von Auskünften

Das Auskunftsrecht

Das Datenschutzrecht gewährt Personen, deren Daten verarbeitet werden, umfassende Rechte (siehe hierzu allgemein Kapitel 3 „Formelle Pflichten – Ein Überblick“, S. 9). Eines dieser Rechte ist das Auskunftsrecht. Das Auskunftsrecht ist in Art. 15 der Europäischen Datenschutz-Grundverordnung (DSGVO) geregelt und durch die jeweiligen Landesdatenschutzgesetze ergänzt.

Hiernach haben Betroffene das Recht, von der datenverarbeitenden Stelle eine Bestätigung zu verlangen, ob über sie personenbezogene Daten gespeichert sind oder verarbeitet werden. Ist das der Fall, hat die Stelle Auskunft über diese Daten sowie weitere Informationen zu erteilen. In der Praxis sind solche Auskunftsanfragen i.d.R. sowohl von Mitgliedsbetrieben, die in die Handwerksrolle als auch von Lehrlingen, die in der Lehrlingsrolle eingetragen sind, zu erwarten. Siehe zur Handwerksrolle Kapitel 9 „Rechtskonforme Verwendung von Daten aus der Handwerksrolle“ (S. 26) und zur Lehrlingsrolle Kapitel 10 „Rechtssicherer Umgang mit Daten aus der Lehrlingsrolle“ (S. 29).

Die Anforderungen an die Erteilung einer Auskunft sind für öffentliche und nicht öffentliche Stellen nahezu identisch, so dass die Ausführungen auch für nicht öffentliche Handwerksorganisationen herangezogen werden können.

Auskunftsersuchen

Die Erteilung der Auskunft setzt zunächst ein Auskunftsersuchen voraus. Die Anfrage kann mündlich, schriftlich oder elektronisch (z.B. per E-Mail) gestellt werden. Zudem sollte das Auskunftsersuchen auf bestimmte Daten oder Informationen präzisiert sein. Dies ist jedoch keine Pflicht. Es kann auch pauschal Auskunft über alle gespeicherten Daten verlangt werden.

Inhalt der Auskunft

Verlangt der Antragsteller eine pauschale Auskunft über seine Daten, sind sämtliche vom Gesetz vorgesehene Informationen zu erteilen. Dies sind im Einzelnen:

- Alle über den Betroffenen gespeicherten Daten (z.B. Name, Anschrift, E-Mail-Adresse, Bankverbindung).

- Die Kategorien der Daten, die verarbeitet werden (z.B. Adress- und Kontaktdaten, Beitragsdaten).

- Die Bezeichnung der Datei (z.B. Handwerksrolle, Lehrlingsrolle, Mitgliederverzeichnis).

- Angaben über die Herkunft der Daten (z.B. Daten wurden beim Betroffenen selbst erhoben, Daten wurden von einer anderen öffentlichen Stelle – z.B. Gewerbeamt – übermittelt).

- Die Empfänger, denen die Daten offengelegt oder zur Nutzung zur Verfügung gestellt wurden (z.B. öffentliche und nicht öffentliche Stellen, die Auskunft aus der Handwerksrolle begehren).

- Die geplante Dauer, für die die Daten gespeichert werden (i.d.R. sind Daten so lange zu speichern, bis sie nicht mehr benötigt werden).

- Der Zweck der Speicherung, d.h. aus welchem Grund werden die Daten gespeichert? (Z.B. Erhebung von Mitgliedsbeiträgen).

Zusätzlich zu den vorgenannten Angaben über die gespeicherten Daten, sind u.a. weitere Informationen zu den Rechten des Betroffenen zu erteilen:

- Hinweis auf das Bestehen eines Rechts auf Berichtigung oder Löschung (Art. 16 DSGVO) oder auf eine Einschränkung der Verarbeitung (Art. 18 DSGVO). Siehe hierzu Kapitel 3 „Formelle Pflichten – Ein Überblick“, S. 9).

- Das Bestehen eines Beschwerderechts des Betroffenen bei der Datenschutzaufsichtsbehörde.

Verfahren der Auskunftserteilung

Die Handwerksorganisation hat sich vor Erteilung der Auskunft über die Identität des Antragstellers zu vergewissern. Der Antragsteller und die betroffene Person, deren Daten gespeichert sind, müssen identisch sein. Wie die Identitätsprüfung erfolgt, bestimmt die Handwerksorganisation.

Wie ist die Auskunft zu erteilen?

Die Auskunft soll wie sämtliche Angaben und Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen (Art. 12 DSGVO).

Die Handwerksorganisation hat dem Antragsteller eine Kopie der Daten zur Verfügung zu stellen. Stellt die betroffene Person den Antrag elektronisch, sind die Informationen in einem gängigen elektronischen Format auszuhändigen. Alternativ kann dem Antragsteller auch ein unmittelbarer Fernzugriff auf die Daten ermöglicht werden.

Kann die Auskunft insgesamt verweigert werden?

Eine Verweigerung der Auskunft kommt nur in Betracht, wenn die Auskunft unmöglich oder mit einem unverhältnismäßigen Aufwand verbunden ist. Dies dürfte für gewöhnlich jedoch nicht der Fall sein. Wird die Auskunft verweigert, ist dies detailliert zu begründen.

In welchem Zeitrahmen ist die Auskunft zu erteilen?

Die Auskunft ist unverzüglich, spätestens innerhalb von vier Wochen, zu erteilen.

Kosten der Auskunft

Die Auskunftserteilung ist für den Betroffenen kostenlos. Verlangt der Antragsteller jedoch mehr als eine Kopie, kann auf Grundlage der Verwaltungskosten ein entsprechendes Entgelt verlangt werden.

Muster zur Auskunftserteilung

Ein Muster zur Erteilung einer Auskunft an einen Mitgliedsbetrieb befindet sich in **Anlage 3**. **Anlage 4** umfasst ein Muster zur Erteilung einer Auskunft an einen Lehrling.

6. Dokumentationspflicht

Weshalb ist eine Dokumentation nötig?

Handwerksorganisationen, die personenbezogene Daten verarbeiten, sind verpflichtet, sämtliche Verarbeitungsprozesse im sogenannten „Verzeichnis von Verarbeitungstätigkeiten“ zu dokumentieren. Hierdurch soll eine Übersicht über die datenschutzrelevanten Abläufe in der Innung, Kreishandwerkerschaft oder der Handwerkskammer gegeben werden. Auf Grundlage dieser Übersicht soll sich die Geschäftsführung über das Ausmaß und die Intensität der Datenverarbeitung in der jeweiligen Organisation bewusst werden.

Die Pflicht zur Dokumentation der Datenverarbeitungsprozesse sowie die konkreten Anforderungen an die Dokumentation sind für private und öffentliche Stellen einheitlich in Artikel 30 der Europäischen Datenschutz-Grundverordnung (DSGVO) geregelt. Weitere Ergänzungen in den Landesdatenschutzgesetzen gibt es nicht.

Was ist zu dokumentieren?

Nach Art. 30 DSGVO sind alle Tätigkeiten zu dokumentieren, bei denen personenbezogene Daten verarbeitet werden. Solche Tätigkeiten können in den unterschiedlichsten Situationen vorkommen (z.B. Erstellung und Veränderung der Mitgliederdateien bzw. Handwerksrolle, Verwaltung der Mitarbeiterakten, Verwendung einer Kamera auf dem Gelände der Handwerksorganisation).

Wie ist der Ablauf der Dokumentation?

Schritt 1: Risikobewertung

Im ersten Schritt ist zu bewerten, ob die Datenverarbeitung ein hohes oder geringes Risiko für die Personen birgt, deren Daten verarbeitet werden. Ein hohes Risiko liegt u.a. dann vor, wenn sehr viele Personen von der Datenverarbeitung betroffen sind (z.B. Videoüberwachung des Innungsgeländes mit Blick auf eine öffentliche Straße). Das gleiche gilt, wenn besonders schutzwürdige Daten (z.B. Gesundheitsdaten, ethnische Herkunft, religiöse Zugehörigkeit) umfangreich verarbeitet werden. Dies ist bei Handwerksorganisationen in der Regel nicht der Fall. Jedoch kann je nach Umfang und Ausmaß bei ESF-Förderungen (Nennung von Migrationshintergrund und Behinderung) oder im Rahmen des Personalwesens (Kirchenzugehörigkeit, Gesundheitsdaten) ein hohes Risiko bestehen.

Sollte ausnahmsweise ein hohes Risiko bestehen, ist eine „Datenschutz-Folgenabschätzung“ vorzunehmen. Die Anforderungen an die Folgenabschätzung richten sich nach Art. 35 DSGVO und umfassen folgende Prüfungspunkte:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge,
- eine Beschreibung Verarbeitungszwecke,
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck,
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen,
- die zur Risikobewältigung und Sicherstellung des Datenschutzes geplanten Maßnahmen.

Schritt 2: Erstellen des Verarbeitungsverzeichnisses

Art. 30 DSGVO zählt die Punkte auf, die in einem Verarbeitungsverzeichnis enthalten sein müssen. Dies sind im Einzelnen:

- **Name und die Kontaktdaten der Organisation** sowie die Namen ihrer Vertreter (z.B. Präsident, Obermeister, Hauptgeschäftsführer etc.).
- **Name und Kontaktdaten des Datenschutzbeauftragten.**
- **Zwecke der Verarbeitung**: Z.B. Erfüllung der gesetzlichen Aufgaben unter Angabe des Paragraphen der HwO.
- Beschreibung der **Kategorien betroffener Personen**: Z.B. Mitglieder, Ansprechpartner aus Verwaltung und Politik, Mitarbeiter etc.
- Beschreibung der **Kategorien personenbezogener Daten**: Werden z.B. einfache Adressdaten oder besonders sensible Daten wie z.B. Gesundheitsdaten erhoben?
- **Kategorien von Empfängern**, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden: Gilt nur, wenn die Daten an Dritte weitergeleitet werden (z.B. Weitergabe von Daten an andere öffentliche Stellen).
- Wenn möglich, die vorgesehenen **Fristen für die Löschung** der verschiedenen Datenkategorien: In der Regel gilt, dass Daten zu löschen sind, wenn sie für den Zweck, für den sie erhoben wurden, nicht mehr benötigt werden.
- Wenn möglich, eine Beschreibung der **technischen und organisatorischen Maßnahmen** (siehe hierzu nachfolgend).

Technische und organisatorische Maßnahmen

Handwerksorganisationen sind verpflichtet, Maßnahmen auf dem Stand der Technik zu ergreifen, um den Risiken zu begegnen, die mit der Datenverarbeitung einhergehen. § 64 Bundesdatenschutzgesetz zählt zahlreiche Maßnahmen auf. Diese lassen sich thematisch auf folgende Kernmaßnahmen zusammenfassen:

- **Vertraulichkeit der Datenverarbeitung (u.a. Zutritts-, Zugangs-, Speicher- und Datenträgerkontrolle)**
  Maßnahmen, die geeignet sind, Unbefugten den Zugang zu Datenverarbeitungsanlagen zu verwehren (z.B. Abschließen des Serverraums).

- **Integrität der Datenverarbeitung (u.a. Eingabekontrolle/ Verarbeitungskontrolle)**
  Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (z.B. Verwendung individueller Benutzernamen).

- **Verfügbarkeitskontrolle**
  Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind und im Störfall wieder hergestellt werden können (z.B. Verwendung von Geräten zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen).

- **Trennungsgebot**
  Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (z.B. Trennung von Daten verschiedener Auftraggeber).

Muster eines Verarbeitungsverzeichnisses

Ein Muster für ein Verarbeitungsverzeichnis ist als **Anlage 5** beigefügt. **Anlage 6** enthält ein ausgefülltes Beispiel. **Anlage 7** umfasst eine Checkliste technischer und organisatorischer Maßnahmen.

7. Der behördliche Datenschutzbeauftragte (DSB)

Gesetzliche Verpflichtung

Die Anforderungen an den behördlichen Datenschutzbeauftragten sind gesetzlich abschließend geregelt. Für die öffentlich-rechtlichen Handwerksorganisationen sind die Artikel 37 bis 39 der Europäischen Datenschutz-Grundverordnung (DSGVO) sowie die jeweiligen Regelungen der Landesdatenschutzgesetze einschlägig.

Welche Handwerksorganisation muss einen Datenschutzbeauftragten benennen?

Alle öffentlichen Stellen müssen einen behördlichen DSB benennen. Dementsprechend sind sämtliche Handwerksammern, Kreishandwerkerschaften und Innungen zur Bestellung verpflichtet. Anders als bisher können jedoch mehrere öffentliche Stellen unter Umständen einen gemeinsamen DSB benennen.

Praxistipp: Die Benennung eines DSB für mehrere Stellen ist insbesondere für Innungen interessant. Hierbei ist zu beachten, dass zum einen die Anzahl der beteiligten Innungen nur so hoch sein darf, dass ein DSB seine Aufgaben bei jeder Innung realistisch erfüllen kann. Zum anderen darf für Innungen kein Mitarbeiter der Handwerkskammer zum DSB bestellt werden, da die Handwerkskammer zugleich Aufsichtsbehörde der Innungen ist.

Wer kann zum DSB benannt werden?

Der DSB kann sowohl ein Mitarbeiter der öffentlichen Stelle (= interner DSB) oder ein außenstehender Dienstleister (= externer DSB) sein.

Unabhängig davon, ob es sich um einen internen oder externen DSB handelt, dürfen nur solche Personen bestellt werden, die

- fachliche Qualifikationen auf dem Gebiet des Datenschutzes besitzen (Datenschutzrecht und IT-Fachwissen) und
- bei der Aufgabenwahrnehmung in keinen Interessenskonflikt geraten können (Interessenskonflikte bestehen z.B. für Mitglieder des Vorstands oder der Geschäftsführung, Leiter der EDV oder der Personalabteilung, etc., da diese Personen für die Datenverarbeitung verantwortlich sind und sich als DSB selbst kontrollieren würden).

Welche Formalien sind zu beachten?

Eine bestimmte Form oder Dauer für die Bestellung sehen die gesetzlichen Regelungen nicht vor. Allein aus Nachweisgründen sollte die Bestellung in Textform erfolgen (siehe hierfür das Muster in **Anhang 8**).

Nach der Bestellung sind jedoch neue Informationspflichten zu beachten:

- Die Kontaktdaten des DSB (z.B. E-Mail-Adresse, Durchwahlnummer, etc.) sind zu veröffentlichen (z.B. auf der Webseite der Handwerksorganisation).

- Die Kontaktdaten des DSB sind der jeweiligen Landesdatenschutzbehörde zu melden.

Wichtig ist, dass nur über die Kontaktdaten zu informieren ist. Dies umfasst nicht zwingend den Namen des DSB.

Praxistipp: Um den Verwaltungsaufwand bei Bestellung eines neuen DSB möglichst gering zu halten und eine erneute Veröffentlichung und Meldung an die Aufsichtsbehörde zu vermeiden, sollten allgemeine Kontaktadressen wie z.B. datenschutzbeauftragter@hwk-xy.de oder datenschutz@kh-xy.de verwendet werden.

Wie ist die Stellung eines DSB?

Ein DSB ist bezüglich seiner Aufgabenerfüllung weisungsunabhängig. Er berichtet unmittelbar der Geschäftsführung und ist bei allen datenschutzrechtlichen Themen frühzeitig einzubinden.

Ein interner DSB darf wegen der Erfüllung seiner Aufgaben weder abberufen noch benachteiligt werden. Für seine zusätzliche Funktion als DSB sind ihm die notwendige Zeit und Unterstützung (z.B. Fortbildung, Ausstattung) zu geben. Ein interner DSB unterliegt zudem einem besonderen Kündigungsschutz. Das Arbeitsverhältnis darf während der Tätigkeit als DSB und für ein Jahr danach nicht gekündigt werden, es sei denn, die Kündigung erfolgt aus wichtigem Grund.

Ein externer DSB gehört nicht der öffentlichen Stelle an. Infolgedessen gelten für ihn die besonderen Kündigungsschutzregeln nicht. Zudem kann der Dienstleistungsvertrag mit einem externen DSB grundsätzlich jederzeit gekündigt werden, soweit vertraglich nicht etwas anderes vereinbart wird.

Welche Aufgaben hat ein DSB zu erfüllen?

Einem DSB obliegen insbesondere folgende Aufgaben:

- Unterrichtung und Beratung sowohl der Geschäftsführung als auch der Mitarbeiter zu allen Belangen des Datenschutzes.
- Überwachung der Einhaltung der Datenschutzvorschriften.
- Sensibilisierung und Schulung der Mitarbeiter.
- Beratung und Überwachung der Durchführung von Datenschutz-Folgenabschätzungen (siehe hierzu Kapitel 6 „Dokumentationspflicht“, S. 18).
- Zusammenarbeit mit der Landesdatenschutzaufsichtsbehörde.
- Ansprechpartner für externe und interne betroffene Personen zu allen Fragen zur Verarbeitung ihrer personenbezogenen Daten.

Welche Verantwortung trifft einen DSB?

Ein DSB ist für die ordnungsgemäße Erfüllung seiner gesetzlichen Aufgaben verantwortlich. Darüber hinausgehende Pflichten oder Haftungsrisiken bestehen nicht. Dies gilt insbesondere für die Einhaltung der datenschutzrechtlichen Vorschriften. Die Geschäftsführung bleibt trotz Benennung eines DSB für das rechtmäßige Handeln der Handwerksorganisation in Datenschutzangelegenheiten verantwortlich. Einen DSB trifft insoweit lediglich die Pflicht zur ordnungsgemäßen Beratung.

Welche Folgen drohen bei Nichtbestellung?

Die DSGVO sieht zwar im Fall einer vorsätzlichen oder fahrlässigen Nichtbestellung erhebliche Bußgelder vor. Der Bundesgesetzgeber hat jedoch von seinem Gestaltungsspielraum Gebrauch gemacht und nimmt öffentliche Stellen des Bundes hiervon aus. Ob und inwieweit die Landesgesetzgeber dieser Ausnahme folgen, ergibt sich aus den jeweiligen Landesdatenschutzgesetzen.

8. Auftragsverarbeitung

Was ist eine Auftragsverarbeitung?

Eine Auftragsverarbeitung liegt vor, wenn eine öffentliche Stelle personenbezogene Daten zwar für ihre Zwecke nutzt, die tatsächliche Verarbeitung und Aufbereitung dieser Daten aber nicht selbst durchführt, sondern von einem Dienstleister vornehmen lässt. Der externe Dienstleister verarbeitet die Daten für und im Auftrag der öffentlichen Stelle. Dies ist z.B. bei Anbietern von Cloud-Lösungen der Fall, die auf ihren Servern Daten für die öffentliche Stelle speichern.

Ist die Auftragsverarbeitung gesetzlich geregelt?

Die Auftragsverarbeitung ist hauptsächlich in Art. 28 der Datenschutz-Grundverordnung (DSGVO) geregelt. Darüber hinaus enthält die DSGVO vereinzelte Vorschriften, die jedoch für Handwerksorganisationen nicht einschlägig sind.

Der Dienstleister wird als „Auftragsverarbeiter“ bezeichnet. Die beauftragende öffentliche Stelle wird „Verantwortlicher“ genannt, da sie die Daten nutzt und damit trotz Einschaltung eines Dienstleisters auch für die Rechtmäßigkeit der Datenverarbeitung einstehen muss und verantwortlich bleibt. Bei Datenschutzverstößen haften Auftragsverarbeiter und Verantwortlicher gemeinsam.

Ist bei der Auftragsverarbeitung eine besondere Form zu beachten?

Art. 28 DSGVO schreibt nicht vor, dass mit dem Auftragsverarbeiter ein Vertrag geschlossen werden muss. In der Praxis ist es jedoch allein wegen der Dokumentation und aus Beweisgründen empfehlenswert, einen Vertrag zu schließen. Eine bestimmte Form ist hierbei nicht einzuhalten. So kann der Vertrag in elektronischen Formaten (z.B. PDF) oder schriftlich in Papierform geschlossen werden.

Welchen Inhalt muss eine Auftragsverarbeitung umfassen?

Art. 28 DSGVO normiert zahlreiche Mindestanforderung an den festzulegenden Inhalt einer Auftragsverarbeitung. Dies betrifft insbesondere folgende Aspekte:

- Gegenstand des Auftrags
- Dauer des Auftrags

- Zweck der Datenverarbeitung
- Art der zu verarbeitenden Daten
- Kategorien der betroffenen Personen
- Ergreifung der erforderlichen technischen und organisatorischen Maßnahmen
- Umfang der Weisungsbefugnisse
- Rückgabe von Datenträgern nach Beendigung des Auftrags

Muster einer Auftragsverarbeitung

Neben den wesentlichen Aspekten eines Auftragsverarbeitungsvertrags sind weitere Punkte vertraglich zu regeln. Es empfiehlt sich deshalb das Vertragsmuster in **Anlage 9** zu verwenden.

9. Rechtskonforme Verwendung von Daten aus der Handwerksrolle

Was erlaubt die Handwerksordnung?

Die Handwerksordnung (HwO) enthält verschiedene Vorschriften zum Datenschutz. Auch für die Verarbeitung von Daten aus der Handwerksrolle gibt es mit § 6 HwO eine konkrete Vorschrift. Die besonderen datenschutzrechtlichen Regeln über Daten aus der Handwerksrolle dürfen jedoch nicht mit den Vorschriften über den Umgang mit Daten aus der Lehrlingsrolle verwechselt oder gleichgesetzt werden. Bei der Weitergabe von Daten aus der Lehrlingsrolle gilt die spezielle Vorschrift des § 28 HwO. Siehe hierzu Kapitel 10 „Rechtssicherer Umgang mit Daten aus der Lehrlingsrolle“, S. 29.

Speicherung von Daten

§ 6 Absatz 1 HwO erlaubt zunächst die Speicherung bestimmter Daten in der Handwerksrolle. Welche Daten gespeichert werden dürfen, ist im Abschnitt I der Anlage D aufgeführt. Anders als bisher erlaubt die Anlage D nun u.a. auch die Erhebung und Speicherung der

- Wohnanschrift von Betriebsinhaber und Betriebsleiter,
- elektronischen Kontaktdaten von Betriebsinhaber und Betriebsleiter (z.B. E-Mail-Adresse, Webseite, Telefaxnummer oder Telefonnummer),
- Bezeichnung, mit der der Betrieb zwar nicht im Handelsregister eingetragen ist, mit der er aber im Geschäftsverkehr auftritt (sog. Etablissementbezeichnung).

Erteilung von Auskünften

§ 6 HwO erlaubt neben der Speicherung zusätzlich die Erteilung von Auskünften aus der Handwerksrolle. Hierbei werden die gespeicherten Daten an Dritte übermittelt. Dritte sind allerdings nur solche Personen und Einrichtungen, die nicht zur Handwerkskammer gehören, also rechtlich selbständig und selbst für die Ordnungsgemäßheit der Datennutzung verantwortlich sind. Die verschiedenen Fachabteilungen der Handwerkskammern sind damit keine Dritten. Der Austausch von Rollendaten zwischen den Abteilungen derselben Handwerkskammer stellt deshalb keine Übermittlung von Daten dar. Die Anforderungen des § 6 HwO sind in diesen Fällen nicht zu beachten. Die Zulässigkeit einer solchen kammerinternen Nutzung von Rollendaten richtet sich dagegen nach den jeweiligen Landesdatenschutzgesetzen.

Wann dürfen Daten aus der Handwerksrolle an Dritte weitergegeben werden?

Die Voraussetzungen einer zulässigen Auskunft aus der Handwerksrolle richten sich maßgeblich danach, ob eine Privatperson bzw. ein Betrieb oder eine öffentliche Einrichtung Auskunft begehrt.

Sollen Daten an eine private Stelle ausgehändigt werden, muss der Antragssteller ein berechtigtes Interesse lediglich glaubhaft darlegen. Ein berechtigtes Interesse ist bei jedem wirtschaftlichen oder ideellen Interesse gegeben und unterliegt keinen weiteren inhaltlichen Anforderungen. Die Darlegung eines berechtigten Interesses genügt auch bei Antrag einer listenmäßigen Auskunft, d.h. einer Vielzahl an Datensätzen, die aufgrund eines bestimmten gemeinsamen Merkmals (z.B. Gewerk oder Postleitzahl) zusammengestellt werden.

Die listenmäßige Auskunft aus der Handwerksrolle darf jedoch selbst bei Vorliegen eines berechtigten Interesses in zwei Fällen nicht erteilt werden. Zum einen ist eine solche umfassende Auskunft untersagt, wenn diejenigen, deren Daten ausgehändigt werden sollen, ein schutzwürdiges Interesse an der Zurückhaltung der Daten haben. Eine Abwägung des schutzwürdigen Interesses der Betroffenen mit dem berechtigten Interesse des Antragstellers ist nicht vorzunehmen. Es genügt, dass ein schutzwürdiges Interesse besteht.

Zum anderen ist eine Auskunft von Rollendaten untersagt, wenn die Betroffenen der Datenweitergabe widersprochen haben. Der Widerspruch zur Weitergabe steht jedem Betrieb zu, der in der Handwerksrolle eingetragen ist. Erklärt ein Betrieb den Widerspruch (Sperrvermerk), dann ist die listenmäßige Weitergabe dieser Daten unzulässig.

Bezüglich der neu eingeführten Möglichkeit zur Erhebung elektronischer Kontaktdaten und der Wohnanschriften des Betriebsinhabers und des Betriebsleiters ist eine Auskunft an private Stellen grundsätzlich untersagt. Etwas anderes gilt nur dann, wenn die Privatadresse und/oder die elektronischen Kontaktdaten zugleich die geschäftliche Anschrift und Kontaktdaten des Betriebs sind. In diesem Fall sind die Daten als Geschäftsdaten zu behandeln.

Begehrt nicht eine Privatperson, sondern eine öffentliche Stelle Auskunft aus der Handwerksrolle, ist dies nur dann erlaubt, soweit die Kenntnis dieser Daten zur Erfüllung der Aufgaben der öffentlichen Stelle erforderlich ist. Liegt die Voraussetzung vor, steht auch ein Sperrvermerk der Datenübermittlung nicht entgegen. Auch das Verbot zur Weitergabe der Wohnanschrift und der elektronischen Kontaktdaten gilt in diesem Zusammenhang nicht.

§ 6 HwO gilt nur für Daten von Betrieben zulassungspflichtiger Handwerke. Auf Daten von Betrieben zulassungsfreier Handwerke findet § 6 HwO aber gemäß § 19 Satz 2 HwO entsprechende Anwendung.

Nutzung und Verarbeitung von Rollendaten

Die Handwerkskammern sind berechtigt, die in der Handwerksrolle gespeicherten Daten zu nutzen. Die Rechtsgrundlage hierfür ergibt sich allerdings nicht aus der HwO, sondern aus den Vorschriften der jeweiligen Landesdatenschutzgesetze.

Einbeziehung des Datenschutzbeauftragten

Angesichts der Komplexität der datenschutzrechtlichen Anforderungen empfiehlt es sich, die gängige Nutzungspraxis mit Daten aus der Handwerksrolle mit dem behördlichen Datenschutzbeauftragten Ihrer Handwerkskammer zu besprechen und offene Fragen zu klären.

10. Rechtssicherer Umgang mit Daten aus der Lehrlingsrolle

Was erlaubt die Handwerksordnung?

Die Handwerksordnung (HwO) umfasst verschiedene Regeln zum Datenschutz. Auch für die Daten aus der Lehrlingsrolle gibt es eine konkrete Vorschrift. § 28 HwO erlaubt bei Vorliegen bestimmter Voraussetzungen die Übermittlung von Lehrlingsrollendaten an Dritte.

Dritte sind dabei nur solche Personen und Einrichtungen, die nicht zur Handwerkskammer gehören, also rechtlich selbständig und selbst für die Ordnungsgemäßheit der Datennutzung verantwortlich sind. Auf Fachabteilungen der Handwerkskammern trifft dies i.d.R. nicht zu, so dass ein Austausch zwischen Abteilungen derselben Handwerkskammer keine Übermittlung von Daten darstellt und damit nicht unter § 28 HwO fällt. Die Zulässigkeit einer solchen kammerinternen Weitergabe richtet sich dagegen nach den jeweiligen Landesdatenschutzgesetzen.

Anders verhält es sich bei der Datenübertragung an Bildungszentren, wenn diese z. B. als GmbH organisiert sind (rechtliche Selbständigkeit) und für Datenschutzverfehlungen selbst – und eben nicht die Handwerkskammer – einzustehen haben. Sind bei einem Bildungszentrum diese Umstände gegeben, liegt eine Übertragung von Lehrlingsrollendaten an Dritte im Sinne von § 28 HwO vor. In diesen Fällen darf eine Datenübermittlung nur erfolgen, wenn die Voraussetzungen des § 28 HwO eingehalten werden.

Wann dürfen Lehrlingsrollendaten an Dritte weitergegeben werden?

Daten aus der Lehrlingsrolle dürfen nach Maßgabe von § 28 Abs. 2 HwO an Dritte übermittelt werden, wenn es zur Regelung, Überwachung, Förderung oder zum Nachweis der Berufsausbildung erforderlich ist. Dementsprechend muss die Weitergabe der Berufsausbildung dienen.

Die berufliche Fortbildung ist hiervon nicht erfasst, so dass z. B. die Daten nicht zum Zweck der Bewerbung von Fortbildungsmaßnahmen an Dritte weitergeleitet werden dürfen.

Was ist, wenn die Voraussetzungen nicht vorliegen?

Liegen die vorgenannten Voraussetzungen nicht vor, weil z.B. eine Fortbildung beworben werden soll, kann eine Weitergabe von Lehrlingsrollendaten an Dritte nicht auf § 28 HwO gestützt werden.

In einem solchen Fall ist die einzig verbleibende Möglichkeit die Einwilligung. Hierzu muss von denjenigen Lehrlingen die schriftliche Zustimmung für Datenübertragungen eingeholt werden, deren Daten an Dritte weitergegeben werden sollen.

Die formalen Anforderungen an eine Einwilligungserklärung folgen aus den Landesdatenschutzgesetzen. Ungeachtet weniger Unterschiede im Detail, fordern alle Gesetze, dass Einwilligungen grundsätzlich schriftlich zu erteilen sind.

In allen anderen Fällen gelten die Landesdatenschutzgesetze

§ 28 HwO regelt ausschließlich die Übermittlung von Daten aus der Lehrlingsrolle an Dritte zum Zweck der Berufsausbildung. Wird dagegen keine Weitergabe der Daten, sondern eine andere Nutzung beabsichtigt, hilft die HwO nicht weiter, da sie diesbezüglich keine Regelungen enthält. Dies gilt etwa für die Aktualisierung der Datensätze, die Verwendung der Daten für statistische Zwecke oder die Nutzung der Daten durch die Fachabteilungen der Kammern zur Erteilung von Informationen an die Lehrlinge selbst.

In diesen Fällen finden die Landesdatenschutzgesetze (LDSG) Anwendung. Diese regeln die Zulässigkeit der Erhebung, Verarbeitung und sonstige Nutzung von Daten für sämtliche öffentliche Stellen und Behörden des jeweiligen Bundeslands und sind nicht gezielt auf Handwerkskammern zugeschnitten. Aus diesem Grund sind die Vorschriften, die eine Erhebung, Nutzung, Verarbeitung etc. erlauben, allgemeiner und abstrakter gefasst.

Bei jeder Nutzung von Lehrlingsrollendaten, die keine Weitergabe an Dritte darstellt, ist deshalb zu prüfen, ob eine Vorschrift aus dem LDSG diese Nutzung erlaubt. Ist dies nicht der Fall, ist eine Datennutzung nur rechtmäßig, wenn derjenige, dessen Daten verarbeitet werden sollen, in die Verarbeitung ausdrücklich und schriftlich eingewilligt hat.

Archivierung gelöschter Daten

Zum rechtmäßigen Umgang mit Daten aus der Lehrlingsrolle gehört ebenso die ordnungsgemäße Aufbewahrung der Daten, nachdem die Daten aus der Lehrlingsrolle gelöscht wurden.

Zunächst ist zu beachten, dass nach Maßgabe des § 28 Abs. 5 HwO die in die Lehrlingsrolle eingetragenen Daten eines Lehrlings am Ende desjenigen Jahres zu löschen sind, in dem das Ausbildungsverhältnis beendet wurde, also der Lehrling seine Ausbildung erfolgreich bestanden oder abgebrochen hat.

Der Begriff des Löschens ist in diesem Zusammenhang irritierend, weil die Daten aus der Lehrlingsrolle zwar entfernt, aber nicht endgültig und unwiderruflich vernichtet werden müssen. Die Handwerkskammern sind stattdessen verpflichtet, die aus der Lehrlingsrolle ent-

fernten Daten in eine gesonderte Datei für ehemalige Lehrlingsrolleneinträge zu speichern (§ 28 Abs. 6 HwO). Hierbei handelt es sich im Grunde um ein Archiv.

Die Daten müssen so lange archiviert werden, bis der ehemalige Lehrling die Daten nicht mehr zum Nachweis seiner Ausbildung benötigt. Spätestens müssen die Daten jedoch nach 60 Jahren aus dem Archiv gelöscht werden. In diesem Fall bedeutet die Anordnung der Löschung die tatsächliche Vernichtung der Daten.

Nutzung archivierter Daten

Die Verwendung, Veränderung und sonstige Verarbeitung von archivierten Lehrlingsdaten verhält sich ebenso wie die Nutzung von Daten, die noch in der Lehrlingsrolle eingetragen sind. Dementsprechend dürfen auch archivierte Daten nur dann an Dritte weitergegeben werden, wenn die Voraussetzungen des § 28 Abs. 2 HwO vorliegen. Infolgedessen besteht gleichermaßen bei archivierten Daten die Einschränkung, dass diese Daten nur zum Zweck der Ausbildung übertragen werden dürfen.

Sollen die Daten nicht an Dritte übermittelt, sondern in anderer Weise genutzt werden, sind die Vorschriften der jeweiligen Landesdatenschutzgesetze heranzuziehen. Insoweit gilt auch hier dasselbe wie für Daten aus der Lehrlingsrolle.

Einbeziehung des Datenschutzbeauftragten

Der rechtsichere Umgang mit Daten aus der Lehrlingsrolle verlangt – wie dargestellt – in verschiedenen Situationen eine unterschiedliche rechtliche Grundlage. Es bietet sich deshalb an, die gängige Nutzungspraxis mit Lehrlingsrollendaten mit dem Datenschutzbeauftragten Ihrer Handwerkskammer zu besprechen und offene Fragen zu klären.

Anlagen

Anlage 1 **Anforderungen der datenschutzrechtlichen Einwilligung**

Muster

Einwilligungserklärung

Einwilligung von Lehrlingen (Vorlage in Rahmen von Schulungen)

Um Sie zeitnah, umfassend und individuell informieren zu können, benötigen wir folgende personenbezogene Daten:

Name:
Anschrift:
Geburtsdatum:
E-Mail:
Ausbildungsberuf:

Die mit Ihrer ausdrücklichen Einwilligung erhobenen und gespeicherten Daten werden ausschließlich vom Berufsbildungszentrum der Handwerkskammer und ausschließlich zum Zweck der Information über Weiterbildungs- und Veranstaltungshinweise genutzt. Eine Weitergabe Ihrer Daten an Dritte erfolgt nur, sofern das Berufsbildungszentrum hierzu gesetzlich verpflichtet ist.

Mir ist bekannt, dass ich zur Abgabe der Einwilligungserklärung nicht verpflichtet bin und ich diese Einwilligungserklärung jederzeit mit Wirkung für die Zukunft widerrufen kann. Der Widerruf ist

per E-Mail zu richten an: info@handwerkskammer-xy.de

oder postalisch an: Handwerkskammer XY, Musterstraße 1, 12345 Musterstadt

Der Widerruf bewirkt, dass meine aufgrund dieser Einwilligungserklärung erfassten Daten gelöscht und mir keine Weiterbildungsangebote mehr unterbreitet werden.

Mit der Verwendung der oben angegebenen Daten durch das Berufsbildungszentrum der Handwerkskammer zum Zwecke der Information über aktuelle Fort- und Weiterbildungsangebote aus dem Angebot des Berufsbildungszentrums erkläre ich mich hiermit einverstanden.

_____ _____
Ort, Datum Unterschrift

Die Datenverarbeitung ist für die Zusendung von Informationen erforderlich und beruht auf Artikel 6 Abs. 1 a) DSGVO. 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 sind 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 unseren Datenschutzbeauftragten unter datenschutz@hwk-xy.de oder unter Datenschutzbeauftragter c/o Handwerkskammer XY, Musterstraße 1, 12345 Musterstadt, erreichen. Ihnen steht des Weiteren ein Beschwerderecht bei der Aufsichtsbehörde zu.

Anlage 2

Informationspflichten bei Erhebung personenbezogener Daten

Muster

Information bei Erhebung von Daten beim Betroffenen

Informationen zur Datenerhebung gemäß Artikel 13 DSGVO

Die Handwerksinnung XY, Musterstraße 1, 12345 Musterstadt, Geschäftsführer Herr Mustermann, erhebt und verarbeitet Ihre Daten zur Erfüllung ihrer gesetzlichen Pflichten sowie zum Zweck der Wahrnehmung ihrer Aufgaben, die im öffentlichen Interesse oder in der Ausübung öffentlicher Gewalt erfolgen.

Die Datenerhebung und Datenverarbeitung ist für die Erfüllung unserer Pflichten und die Wahrnehmung unserer Aufgaben erforderlich und beruht auf Artikel 6 Abs. 1 c) und e) DSGVO. Eine Weitergabe Ihrer Daten erfolgt ausschließlich auf gesetzlicher Grundlage an andere öffentliche Stellen, die Ihre Daten zur Erfüllung ihrer gesetzlichen Aufgaben benötigen oder an private Personen, die ein berechtigtes Interesse an der Verwendung Ihrer Daten darlegen. Sofern keine besonderen gesetzlichen Aufbewahrungspflichten bestehen, werden die Daten gelöscht, sobald sie für den Zweck ihrer Verarbeitung nicht mehr erforderlich sind.

Sie haben das Recht, der Verwendung Ihrer Daten zum Zweck der Ausübung unserer Aufgaben, die im öffentlichen Interesse oder in der Ausübung öffentlicher Gewalt liegen, 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 unseren Datenschutzbeauftragten unter datenschutz@handwerksinnung-xy.de oder unter Datenschutzbeauftragter c/o Handwerksinnung XY, Musterstraße 1, 12345 Musterstadt, erreichen.

Ihnen steht des Weiteren ein Beschwerderecht bei der Aufsichtsbehörde zu.

Anlage 2 A

Informationspflicht bei Erhebung personenbezogener Daten auf Webseiten

Beispielsformulierungen zur Ergänzung des Datenschutzhinweises

Die Datenschutzerklärung auf Webseiten richtet sich danach, ob und inwieweit personenbezogene Daten auf der Webseite erhoben werden. Dies kann z.B. durch ein Tracking-Tool, Kontaktformulare oder Bestellungen von Newslettern der Fall sein und muss in jedem Einzelfall individuell angefertigt werden. Für typische Verarbeitungssituationen können Sie folgende Beispielformulierungen verwenden.

Kontaktformular

Wir erheben Ihre Daten zum Zweck der Durchführung Ihrer Kontaktanfrage. Die Datenverarbeitung beruht auf Artikel 6 Abs. 1 f) DSGVO. Unser berechtigtes Interesse ist, Ihre Anfrage zu beantworten. 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 Kontaktaufnahme jederzeit zu widersprechen.

Newsletter

Wir erheben Ihre Daten zum Zweck der Zusendung des von Ihnen gewünschten Informationsmaterials. Die Datenverarbeitung beruht auf Ihrer Einwilligung gemäß Artikel 6 Abs. 1 a) DSGVO. 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 Zusendung von Informationsmaterialien jederzeit zu widersprechen.

Registrierung im Mitgliederbereich

Wir erheben Ihre Daten zum Zweck der Durchführung Ihrer Anmeldung für den Mitgliederbereich von www…..de. Die Datenverarbeitung beruht auf Artikel 6 Abs. 1 f) DSGVO. Wir verfolgen das Interesse, sicherzustellen, dass nur Mitglieder Zugriff auf den Mitgliedern vorbehaltenen Informationen erhalten. 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 Registrierung jederzeit zu widersprechen.

Ihre Rechte

Sie sind 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. Ihnen steht des Weiteren ein Beschwerderecht bei der Aufsichtsbehörde zu.

Datenschutzbeauftragter

Wenn ein Datenschutzbeauftragter benannt werden muss, müssen dessen Kontaktdaten ebenfalls auf der Webseite genannt werden.

Anlage 3

Die Erteilung von Auskünften

Es handelt es sich um ein Muster, das von der jeweiligen Handwerkskammer angepasst werden muss.

MUSTER

Auskunftserteilung an einen eingetragenen Betrieb Datenspeicherung durch die Handwerkskammer

Herrn/Frau
Michael(a) Muster
Mustergasse 1
33333 Musterstadt

Sehr geehrte/r Frau/Herr _____,

Sie haben uns um Auskunft darüber gebeten, welche Daten wir zu Ihrer Person und zu Ihrem Betrieb gespeichert haben. Sie sind bei uns mit Ihrem Betrieb erfasst.

I. Auf Grundlage von § 6 Abs. 1 und § 19 der Handwerksordnung (HwO) in Verbindung mit Anlage D zur Handwerksordnung haben wir die der Tabelle 1 zu entnehmenden Angaben zu Ihrer Person und zu Ihrem Betrieb gespeichert. Diese Daten haben wir von Ihnen oder auf Grundlage von § 14 Abs. 8 Satz 1 Nr. 2 der Gewerbeordnung (GewO) von der zuständigen Gewerbebehörde oder gemäß § 5a Abs. 2 HwO von einer anderen Handwerkskammer erhalten. Zweck der Speicherung dieser Daten ist die Erfüllung der uns nach der HwO übertragenen Aufgaben. Eine Weitergabe der Daten erfolgt ausschließlich auf gesetzlicher Grundlage. Bei der Weitergabe ist zu unterscheiden, ob es sich bei den Empfängern um eine öffentliche oder um eine nicht öffentliche Stelle handelt.

a) Öffentliche Stellen
An öffentliche Stellen werden von uns gem. § 6 Abs. 3 HwO die in der Tabelle 1 genannten Daten weitergegeben, sofern die Kenntnis dieser Daten zur Erfüllung der Aufgaben der anfragenden öffentlichen Stelle erforderlich ist (z.B. Deutsche Rentenversicherung, Gewerbeämter, Handwerkskammern, Kreishandwerkerschaften im jeweils satzungsmäßigen Zuständigkeitsbereich).

b) Nicht öffentliche Stellen
Hinsichtlich der Weitergabe von Daten an nicht öffentliche Stellen werden Einzelauskünfte nach § 6 Abs. 2 HwO jedem erteilt, der ein berechtigtes Interesse glaubhaft darlegt. Eine listenmäßige Weitergabe von Daten wird nach § 6 Abs. 2 HwO erteilt, wenn sie zur Erfüllung

der Aufgaben der Handwerkskammer erforderlich ist oder wenn der Auskunftbegehrende ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und kein Grund zu der Annahme besteht, dass Sie ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung haben bzw. Sie keinen Widerspruch eingelegt haben. Ein Widerspruch liegt uns für …….. vor.

II. Neben den oben angeführten Angaben haben wir für unsere internen Verwaltungszwecke weitere folgende Daten gespeichert:

- Zeitpunkt der letzten Änderung
- Betriebsnummer
- Grundsätzliche Beitragspflicht
- Beitreibgemeinde
- Wahlgruppe und -bezirk bezüglich der Kammerwahlen

Diese Daten wurden von uns selbst angelegt und werden ausschließlich zu Verwaltungszwecken verwendet. Eine Weitergabe an Dritte erfolgt nicht.

III. Gemäß § 106 Abs. 1 Nr. 5 und § 113 HwO sind wir berechtigt, zur Festsetzung der Beiträge Kammerzugehöriger die Bemessungsgrundlagen bei den Finanzbehörden zu erheben. Dementsprechend haben wir von Ihnen die in Tabelle 2 aufgeführten Daten gespeichert. Über diese Daten verfügen wir aufgrund der Übermittlung durch die Finanzämter. Diese Daten werden ausschließlich zum Zweck der Beitragsfestsetzung erhoben und gespeichert. Eine Weitergabe dieser Daten an Dritte erfolgt nicht.

IV. Ergänzend zu internen Verwaltungszwecken haben wir folgende Daten gespeichert:

- Zum Soll gestellte, d.h. veranlagte Grundbeiträge und Umlagen sowie das jeweilige Datum des Bescheids.
- Bezahlte Grundbeiträge und Umlagen sowie das jeweilige Datum der Zahlung sowie die Zahlungswege.

Diese Daten wurden von uns selbst angelegt und werden grundsätzlich ausschließlich zu internen Verwaltungszwecken verwendet. Eine Weitergabe solcher Daten an nicht öffentliche Stellen erfolgt nicht.

Lediglich Angaben über offene Beträge der von uns festgesetzten Beiträge werden gegebenenfalls an öffentliche Stellen weitergegeben, sofern dies zur Erfüllung unserer Aufgaben oder der anfragenden öffentlichen Stelle erforderlich ist. Namentlich sind hier die Fälle der Beitreibung oder Gewerbeuntersagung zu nennen. Andere der genannten Daten werden auch an öffentliche Stellen nicht weitergegeben.

V. Die Handwerkskammer gemäß § 23 HwO i. V. m. §§ 32, 76 BBiG berechtigt, u. a. die Berufsbildung zu überwachen. Zur Erfüllung dieser Aufgabe speichern wir bei Ausbildungsbetrieben zusätzlich die in Tabelle 3 aufgeführten Daten. Die Daten werden ausschließlich zur Erfüllung unserer gesetzlichen Pflichten gespeichert.

Die Handwerkskammer darf zur Verbesserung der Ausbildungsvermittlung, der Aktualität der Ausbildungsstatistik und der besseren Feststellung von Angebot und Nachfrage die folgenden Daten gemäß § 28 HwO an die Bundesagentur für Arbeit übermitteln:

- Namen, Vornamen und Geburtsdaten und Anschrift des Lehrlings
- Namen und Anschrift der Ausbildungsstätte
- Ausbildungsberuf
- Datum und Beginn der Berufsausbildung

VI. Bei ehrenamtlich für die Handwerkskammer tätigen Personen erfolgt eine Speicherung und Verarbeitung personenbezogener Daten, soweit dies für die Wahrung der ehrenamtlichen Tätigkeiten erforderlich ist.

Wir hoffen, dass wir mit den vorstehenden Ausführungen Ihre Fragen hinreichend beantworten konnten. Informieren Sie uns bitte, falls Daten unrichtig sind.

Sie haben das Recht, sich bei der für die Handwerkskammer zuständigen Datenschutzaufsichtsbehörde……(Name, Adresse, E-Mail) zu beschweren, falls Sie der Meinung sind, dass die Verarbeitung Ihrer personenbezogenen Daten nicht rechtmäßig erfolgt.

Für weitere Auskünfte stehen wir Ihnen selbstverständlich gerne zur Verfügung.

Mit freundlichen Grüßen

Handwerkskammer ……..

Anlagen

Tabelle 1: Handwerksrollendaten

	Natürliche Person	Juristische Personen	Personengesellschaften
	Betriebsinhaber	Gesetzliche Vertreter	Für die technische Betriebsleitung verantwortliche persönlich haftender Gesellschafter oder technischer Betriebsleiter
Familienname			
Vorname			
Geburtsname			
Geburtsdatum			
Staatsangehörigkeit			
Firma			
Ort der Niederlassung			
Straße der Niederlassung			
Betriebene Handwerke			
Eintragungsvoraussetzungen			
Art, Ort und Zeitpunkt der Prüfung die zur Ausübung			

des Handwerks berechtigt			
Eintragungszeitpunkt			
		Betriebsleiter	Weitere Gesellschafter
Familienname			
Vorname			
Geburtsname			
Geburtsdatum			
Staatsangehörigkeit			
Vertretungsbefugnis			

Tabelle 2: Beitragsdaten

Beitrag	
Zeitpunkt der letzten Änderung	
Betriebsnummer	
Grundsätzliche Beitragspflichtigkeit	
Beitreibgemeinde	
Wahlgruppe und -bezirk bezüglich der Kammerwahlen	
Finanzamt	
Steuernummer	
Bemessungsgrundlagen, d.h. Gewerbeerträge der Beitragsjahre	
Vorläufige Bemessungsgrundlagen, d.h. Gewerbeerträge, die den vorläufigen Veranlagungen zugrunde liegen.	
Zum Soll gestellte, d.h. veranlagte Grundbeiträge	
Datum des Bescheids	
Zum Soll gestellte Umlagen	
Datum des Bescheids	
Bezahlte Grundbeiträge und Umlagen	
Datum der Zahlung	
Zahlungsweg	

Tabelle 3: Ausbildungsbetrieb

Ausbildungsbetrieb	
Ausbilder	
Familienname	
Vorname	
Geburtsname	
Geburtsdatum	
Art der fachlichen Eignung	
Auszubildende	
Familienname	
Vorname	
Geburtsname	
Geburtsdatum	
Ausbildungsbeginn	
Ausbildungsende	
Prüfungstermine	

Anlage 4

Die Erteilung von Auskünften

Es handelt es sich um ein Muster, das von der jeweiligen Handwerkskammer angepasst werden muss.

MUSTER

Auskunftserteilung an einen Auszubildenden

Herrn/Frau
Michael(a) Muster
Mustergasse 1
33333 Musterstadt

Sehr geehrte/r Frau/Herr _____,

Sie haben uns um Auskunft darüber gebeten, welche Daten wir zu Ihrer Person gespeichert haben. Sie sind bei uns als Lehrling erfasst. Zur Datenverarbeitung durch die Handwerkskammer teilen wir Ihnen folgendes mit.

I. Die Datenerhebung erfolgt auf der Grundlage von § 28 der Handwerksordnung (HwO) in Verbindung mit Anlage D zur Handwerksordnung. Zweck der Speicherung dieser Daten ist die Erfüllung der uns nach der Handwerksordnung gesetzlich übertragenen Aufgaben. Entsprechend dieser Berechtigung haben wir die der beigefügten Tabelle zu entnehmenden Angaben zu Ihrer Person gespeichert.

Die Daten werden am Ende des Kalenderjahres, in dem das Berufsausbildungsverhältnis beendet wird, in der Lehrlingsrolle gelöscht und dann in einer gesonderten Datei höchstens 60 Jahre lang archiviert. Hinsichtlich der Weitergabe dieser Daten ist zwischen der Weitergabe an öffentliche und nicht öffentliche Stellen zu unterscheiden.

Die Daten dürfen an öffentliche und nicht öffentliche Stellen zur Regelung, Überwachung, Förderung und zum Nachweis der Berufsausbildung in anerkannten Ausbildungsberufen übermittelt werden.

a) Öffentliche Stellen
Gem. § 28 Abs. 7 HwO werden zur Regelung, Verbesserung der Ausbildungsvermittlung, zur Verbesserung der Zuverlässigkeit und Aktualität der Ausbildungsvermittlungsstatistik sowie zur Verbesserung der Feststellung von Angebot und Nachfrage auf dem Ausbildungsmarkt folgende Daten aus der Lehrlingsrolle an das statistische Bundesamt und die Bundesagentur für Arbeit übermittelt:

1.Name, Geburtsname, Vorname, Geburtsdatum und Anschrift des Lehrling (Auszubildenden),
2. Name und Anschrift der Ausbildungsstätte,
3. Ausbildungsberuf sowie
4. Datum des Beginns der Berufsausbildung.

Zur Regelung der Ausbildung werden die Daten an die zuständigen Prüfungsausschüsse der Handwerkskammer übermittelt. Die zuständige Innung und der Lehrlingswart erhalten die Daten zur Überwachung und Förderung der Ausbildung.

b) Nicht öffentliche Stellen
Hinsichtlich der Weitergabe von Daten an nicht öffentliche Stellen gilt, dass die Daten der Lehrlingsrolle ausschließlich an ein privatwirtschaftlich betriebenes Berufsbildungszentrum der Handwerkskammer weitergegeben werden.

Wir hoffen, dass wir mit den vorstehenden Ausführungen Ihre Fragen hinreichend beantworten konnten. Informieren Sie uns bitte, falls Daten unrichtig sind.

Sie haben das Recht, sich bei der für die Handwerkskammer zuständigen Datenschutzaufsichtsbehörde ……..(Name, Adresse, E-Mail) zu beschweren, falls Sie der Meinung sind, dass die Verarbeitung Ihrer personenbezogenen Daten nicht rechtmäßig erfolgt.

Für weitere Auskünfte stehen wir Ihnen selbstverständlich gerne zur Verfügung.

Mit freundlichen Grüßen

Handwerkskammer ……..

Anlage

Lehrling	
Familienname	
Vorname	
Geburtsname	
Geschlecht	
Geburtsdatum	
Staatsangehörigkeit	
Straße	
PLZ	
Wohnort	
Allgemeinbildender Schulabschluss	
Vorausgegangene Teilnahme an berufsvorbereitender Qualifizierung oder beruflicher Grundbildung	
Berufliche Vorbildung	
Gesetzlicher Vertreter (falls erforderlich)	
Familienname	
Vorname	
Geburtsname	
Straße	
PLZ	
Wohnort	
Ausbildungsverhältnis	
Ausbildungsberuf & Fachrichtung	
Ausbildungsschwerpunkt	
Datum Abschluss Ausbildungsvertrag	
Ausbildungsdauer	
Datum Beginn Berufsausbildung	
Dauer der Probezeit	

Anlage 5

Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen

Hauptblatt

Angaben zum Verantwortlichen, Art. 30 Abs. 1 a) DSGVO

1. Verantwortlicher (= Firma/Legaleinheit)

2. Gesetzlicher Vertreter (= Präsident, HGF, Obermeister, Geschäftsführung)

3. Datenschutzbeauftragter

Name:

Anschrift:

E-Mail:

Tel.:

4. Zuständige Aufsichtsbehörde
Landesbeauftragter für Datenschutz und Informationsfreiheit Bundesland XY

Verpflichtende Meldung des/der Datenschutzbeauftragten bereits erfolgt:

☐ Ja

☐ Nein

5. Regelungen zur Datensicherheit
IT-Sicherheitskonzept
[Verweis auf übergreifende IT-Sicherheitskonzepte, die grundsätzlich für alle Verarbeitungstätigkeiten gelten]

6. Sachverhalte zu Drittstaatenübermittlungen

Erläuterungen zum Hauptblatt

Nr. 1	Verantwortlicher ist jede Person oder Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DSGVO) Angaben: Name, ladungsfähige Anschrift
Nr. 2	Vorstände, Geschäftsführer Angaben: Namen des Präsidenten, des Hauptgeschäftsführers, des Obermeisters und/oder des Geschäftsführers) *Gegebenenfalls kann hier einfach ein Link auf das Impressum der Webseite des Betriebs eingetragen werden.*
Nr. 3	Vom Verantwortlichen bestellter Datenschutzbeauftragter Angaben: Name, Kontaktdaten
Nr. 4	Die Meldung der Kontakt-Informationen des Datenschutzbeauftragten (Funktions-)E-Mail-Adresse und Telefonnummer sind Pflichtangaben
Nr. 5	Gegebenenfalls Verweise auf übergreifende Regelungen (*falls solche existieren, die grds. alle Verarbeitungen* betreffen) Der Verweis auf übergreifende Regelungen an dieser Stelle entbindet nicht von der Dokumentation von ggf. erforderlichen Abweichungen zu den einzelnen Verarbeitungstätigkeiten. Verweis z.B. auf ein IT-Sicherheitskonzept, das alle Verarbeitungstätigkeiten einschließt. Eventuell auch Verweise auf relevante Dokumente eines ISMS nach ISO27001.
Nr. 6	Ein Verweis zur Regelungen zur Drittstaatenübermittlung ist hier sinnvoll, wenn alle oder die Mehrzahl der Verarbeitungen hierdurch geregelt werden, z.B. durch BCR.

Verzeichnis von Verarbeitungstätigkeiten

Verzeichnis Nr. _____

☐ Ersterstellung

☐ Änderung eines bestehenden Verzeichnisses

Erstellungsdatum:

Bezeichnung der Verarbeitungstätigkeit:

I. Angaben zur Verantwortlichkeit, Art. 30 Abs. 1 b) DSGVO

1. Verantwortlicher Fachbereich/verantwortliche Führungskraft

2. Bei gemeinsamer Verantwortlichkeit:
Name und Kontaktdaten des Leiters/der Leiter oder 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 DSGVO). Datenschutz-Folgenabschätzung als separate Anlage beifügen.

4. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit

5. Rechtsgrundlage der Verarbeitungen/der Verarbeitungstätigkeit

6. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, Art. 30 Abs. 1 c) DSGVO	
6.1. Betroffene Personengruppen	**6.2. Kategorien personenbezogener Daten**

7. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden, Art. 30 Abs. 1 d) DSGVO	
7.1. Interne Empfänger	
7.2. Externe Empfänger	
7.3. Vertragliche Dienstleister (Vertrag der Auftragsdatenverarbeitung als Anlage beifügen)	

8. Datenübermittlungen in Drittländer oder an internationale Organisationen, Art. 30 Abs. 1 e) DSGVO

Übermittlung

☐ Nein

☐ Ja

Wenn ja, dann: Name des Drittlandes / der internationalen Organisation

9. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien, Art. 30 Abs. 1 f) DSGVO

10. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO
10.1. Art der eingesetzten Datenverarbeitungsanlagen und Software (optional)
10.2. Konkrete Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO

----- Optionale Angaben ----

Weitere Dokumentationen zur Verarbeitungstätigkeit

----- Ende Optionale Angaben----

Erläuterungen zum Verarbeitungsverzeichnis

Nr. 1	Eindeutige Bezeichnung der dokumentierten Verarbeitung/ Verarbeitungstätigkeit auf Grundlage eines Fachprozesses. Es sollte eine in der Organisation geläufige Bezeichnung des Fachprozesses gewählt werden. Beispiele: - Allgemeine Kundenverwaltung - Customer-Relationship-Management (CRM)
Nr. 1	Nach der Unternehmensorganisation für die konkrete Verarbeitungstätigkeit verantwortlicher Fachbereich/verantwortliche Führungskraft (*sofern möglich und sinnvoll, zumindest als Funktionsbezeichnung*)
Nr. 2	Falls mehrere Verantwortliche gemeinsam für die Verarbeitungstätigkeiten verantwortlich sind, sind hier Name und Kontaktdaten des/der weiteren Verantwortlichen anzugeben (Firma/ladungsfähige Anschrift; Art. 30 Abs. 1 a) DSGVO, Art. 26 Abs. 1 DSGVO)
Nr. 3	Es ist zu bewerten, ob die Datenverarbeitung ein hohes Risiko für die Personen birgt, deren Daten verarbeitet werden. Ein hohes Risiko liegt u.a. dann vor, wenn sehr viele Personen von der Datenverarbeitung betroffen sind. Das gleiche gilt, wenn besonders schutzwürdige Daten (z.B. Gesundheitsdaten) umfangreich verarbeitet werden.
Nr. 4	Beispiele: - Verarbeitungstätigkeit: „Allgemeine Mitgliederverwaltung"; verfolgte Zweckbestimmungen: „Auftragsbearbeitung, Buchhaltung und Inkasso" - Verarbeitungstätigkeit: „Customer-Relationship-Management"; verfolgte Zweckbestimmungen: „Dokumentation und Verwaltung von Mitgliederbeziehungen, Marketing, Beschwerdemanagement, Kündigungsprozess" Eine Verarbeitungstätigkeit kann mehrere Teil-Geschäftsprozesse zusammenfassen. Dementsprechend kann eine Verarbeitung auch mehrere Zwecke umfassen, so dass auch mehrere Zweckbestimmungen angegeben werden können. Die erforderliche Detailtiefe hängt von der Tätigkeit des Verantwortlichen ab. Es können neben dem Fachprozess auch begleitende mitarbeiterbezogene Unterstützungsprozesse vorliegen wie z.B. zur Personalführung/-einsatzplanung. Diese können entweder als Teil einer anderen Verarbeitung oder als eigene Verarbeitung beschrieben sein.
Nr. 5	Die Nennung der einschlägigen Rechtsgrundlage ist für Rechenschaftspflichten und die Gewährleistung von Transparenzpflichten ggü. den betroffenen Personen notwendig. Die Rechtsgrundlage können z.B. eine gesetzliche Vorschrift oder eine Einwilligung durch den Betroffenen sein.
Nr. 6	Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, Art. 30 Abs. 1 c) DSGVO
Nr. 6.1	Als betroffene Personengruppen kommen beispielsweise Mitglieder, Ar-

	beitnehmer, Schuldner usw. in Betracht.
Nr. 6.2	Den einzelnen Personengruppen sind die jeweils auf sie bezogenen verwendeten Daten oder Datenkategorien zuzuordnen. Damit sind keine personenbezogenen Daten, sondern "Datenbezeichnungen"/Datenkategorien gemeint (z.B. „Adresse“, „Geburtsdatum“, „Bankverbindung“). Werden solche Datenkategorien angegeben, so müssen diese so konkret wie möglich sein. Nicht ausreichend sind etwa Angaben wie „Mitgliederdaten“ oder Ähnliches. Beispiele: - Mitglieder: Adressdaten, Kontaktkoordinaten (einschl. Telefon-, Fax- und E-Mail-Daten), Geburtsdatum, Vertragsdaten, Bonitätsdaten, Betreuungsinformationen einschließlich Kundenentwicklung, Produkt- bzw. Vertragsinteresse, Statistikdaten, Abrechnungs- und Leistungsdaten, Bankverbindung - Beschäftigtendaten (Lohn und Gehalt): Kontaktdaten, Bankverbindung, Sozialversicherungsdaten, etc.
Nr. 7	Empfängerkategorien sind insbesondere am Prozess beteiligte weitere Stellen des Unternehmens oder andere Gruppen von Personen oder Stellen, die Daten – ggf. über Schnittstellen – erhalten z.B. in den Prozess eingebundene weitere Fachabteilungen, Vertragspartner, Mitglieder, Behörden, Versicherungen, Auftragsverarbeiter (z.B. Dienstleistungsrechenzentrum, Call-Center, Datenvernichter, Anwendungsentwicklung, Cloud Service Provider) usw.
Nr. 8	Drittländer sind solche außerhalb der EU/des EWR Beispiele für internationale Organisationen: Institutionen der UNO, der EU. Liegt keine der genannten Garantien vor, sind hier andere getroffene Garantien zu dokumentieren, Art. 49 Abs. 1. UAbs. 2 DSGVO.
Nr. 9	Anzugeben sind hier die konkreten Aufbewahrungs-/Löschfristen, die in Verarbeitungstätigkeiten implementiert sind, bezogen auf einzelne Verarbeitungsschritte, falls unterschiedlich. Soweit diese in einem Löschkonzept dokumentiert sind, reicht der Verweis auf das vorhandene und in der Verarbeitungstätigkeit umgesetzte Löschkonzept aus.
Nr. 10	Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO.
Nr. 10.1	Optional kann an dieser Stelle eine knappe Beschreibung der technischen Infrastruktur wie der technischen und organisatorischen Sicherheitsmaßnahmen angegeben werden, um ein besseres Verständnis der allgemeinen Beschreibung der technischen und organisatorischen Maßnahmen (siehe 10.2.) zu ermöglichen.
Nr. 10.2	Soweit sich die technischen und organisatorischen Maßnahmen schon aus vorhandenen Sicherheitsrichtlinien/Konzepten/Zertifizierungen ergeben, ist ein konkreter Verweis hierauf ausreichend. Insbesondere sind hier Abweichungen zu einem übergreifenden Sicherheitskonzept (**siehe Hauptblatt Nr. 5**) zu dokumentieren. Wenn eine Datenschutz-Folgenabschätzung für die Verarbeitung hohe Risiken ausweist,

	so sind die zur Bewältigung dieser Risiken getroffenen Sicherheitsvorkehrungen für die Verarbeitung in der Datenschutz-Folgenabschätzung zu dokumentieren, Art. 35 Abs. 7 d) DSGVO. Ein Verweis auf das Vorhandensein einer Datenschutz-Folgenabschätzung ist eine sinnvolle optionale Angabe (siehe unten).
Optional	Im Hinblick auf die vielfältigen Nachweispflichten, denen die Organisation im Datenschutz unterliegt, kann es sinnvoll sein, weitere Aspekte zur Verarbeitungstätigkeit zu dokumentieren. Diese sind nur intern zu verwenden. Zu diesen zusätzlichen Dokumentationen, die sinnvollerweise hier erfolgen, gehören z. B. • *Angaben zur Zusammenstellung der Informationspflichten (insbes. Art. 13,14 DSGVO)* • *Verträge mit Dienstleistern (Art. 28 DSGVO)* • *Vereinbarungen zur gemeinsamen Verantwortung (Art. 26 DSGVO)* • *Eine Bewertung der Risiken der Verarbeitungstätigkeit für die Rechte und Freiheiten natürlicher Personen* • *durchgeführte Datenschutzfolgeabschätzungen zur Verarbeitungstätigkeit oder einzelnen Verarbeitungsschritten (Art. 35 DSGVO)*

Anlage 6

Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen

Hauptblatt

Angaben zum Verantwortlichen, Art. 30 Abs. 1 a) DSGVO

1. Verantwortlicher (= Firma/Legaleinheit)
Handwerkskammer Musterstadt, Musterstraße 17-21, 12345 Musterstadt

2. Gesetzlicher Vertreter (= Präsident, HGF, Obermeister, Geschäftsführung)
Herr Mustermann, Musterstraße 17-21, 12345 Musterstadt

3. Datenschutzbeauftragter

Name: Frau Anja Mustermann

Anschrift: Musterstraße 17-21,12345 Musterstadt

E-Mail: datenschutzbeauftragter@hwk-musterstadt.de

Tel.: 01234/ 123456-34

4. Zuständige Aufsichtsbehörde
Landesbeauftragter für Datenschutz und Informationsfreiheit des Landes XY

Verpflichtende Meldung des/der Datenschutzbeauftragten bereits erfolgt:

☒ Ja
☐ Nein

5. Regelungen zur Datensicherheit
IT-Sicherheitskonzept der HwK Musterstadt

6. Sachverhalte zu Drittstaatenübermittlungen
Findet nicht statt.

Erläuterungen zum Hauptblatt

Nr. 1	Verantwortlicher ist jede Person oder Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DSGVO) Angaben: Name, ladungsfähige Anschrift
Nr. 2	Vorstände, Geschäftsführer Angaben: Namen des Präsidenten, des Hauptgeschäftsführers, des Obermeisters und/oder des Geschäftsführers) *Gegebenenfalls kann hier einfach ein Link auf das Impressum der Webseite des Betriebs eingetragen werden.*
Nr. 3	Vom Verantwortlichen bestellter Datenschutzbeauftragter Angaben: Name, Kontaktdaten
Nr. 4	Die Meldung der Kontakt-Informationen des Datenschutzbeauftragten (Funktions-)E-Mail-Adresse und Telefonnummer sind Pflichtangaben
Nr. 5	Gegebenenfalls Verweise auf übergreifende Regelungen (*falls solche existieren, die grds. alle Verarbeitungen* betreffen) Der Verweis auf übergreifende Regelungen an dieser Stelle entbindet nicht von der Dokumentation von ggf. erforderlichen Abweichungen zu den einzelnen Verarbeitungstätigkeiten. Verweis z.B. auf ein IT-Sicherheitskonzept, das alle Verarbeitungstätigkeiten einschließt. Eventuell auch Verweise auf relevante Dokumente eines ISMS nach ISO27001.
Nr. 6	Ein Verweis zur Regelungen zur Drittstaatenübermittlung ist hier sinnvoll, wenn alle oder die Mehrzahl der Verarbeitungen hierdurch geregelt werden, z.B. durch BCR.

Verzeichnis von Verarbeitungstätigkeiten

Verzeichnis Nr. 1

☒ Ersterstellung

☐ Änderung eines bestehenden Verzeichnisses

Erstellungsdatum: 21.8.2017

Bezeichnung der Verarbeitungstätigkeit: Führung der Handwerksrolle

I. Angaben zur Verantwortlichkeit, Art. 30 Abs. 1 b) DSGVO

1. Verantwortlicher Fachbereich/verantwortliche Führungskraft
Herr 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 DSGVO). Datenschutz-Folgenabschätzung als separate Anlage beifügen.

4. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit
Führung der Mitgliederverzeichnisse der Handwerkskammer Musterstadt

5. Rechtsgrundlage der Verarbeitungen/der Verarbeitungstätigkeit
§§ 6, 18, 19 HwO, Anlage D HwO

6. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, Art. 30 Abs. 1 c) DSGVO	
6.1. Betroffene Personengruppen	**6.2. Kategorien personenbezogener Daten**
Betriebsinhaber	Name, Vorname, Adressdaten, Geburtsdatum, Geburtsort, Geschlecht, Qualifikation, Prüfungsdaten, (elektronische) Kontaktdaten, ggfs. Firma oder Etablissementbezeichnung
Technische Betriebsleiter	Siehe oben
Ausbilder?	Siehe oben (ohne Adressdaten)

7. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden, Art. 30 Abs. 1 d) DSGVO)	
7.1. Interne Empfänger	Mitarbeiter der Abteilung Handwerksrolle und Beitrag
7.2. Externe Empfänger	Partielle Offenlegung ggü. der DRV, den SOKAs der jeweiligen Handwerke, örtlich zuständigen Energieversorgern
7.3. Vertragliche Dienstleister (Vertrag der Auftragsdatenverarbeitung als Anlage beifügen)	Externer EDV-Dienstleister für die Führung der Datenbank, Dienstleister für die Führung der Betriebssuche.

8. Datenübermittlungen in Drittländer oder internationale Organisationen, Art. 30 Abs. 1 e) DSGVO

Übermittlung

☒ Nein

□ Ja

Wenn ja, dann: Name des Drittlandes / der internationalen Organisation (DSGVO)

9. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien, Art. 30 Abs. 1 f) DSGVO Löschfristen ergeben sich aus § 13 Abs. 5 HwO, d.h. 30 Jahre nach der Löschung des Betriebes aus der Handwerksrolle.

10. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO IT-Sicherheitskonzept der HWK Musterstadt
10.1. Art der eingesetzten Datenverarbeitungsanlagen und Software (optional) - DV-Anlagen - Software (und ggf. Unterprogramme) - Schnittstellen
10.2 Konkrete Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO ---------- *(Siehe IT-Sicherheitskonzept)*

----- Optionale Angaben ----

Weitere Dokumentationen zur Verarbeitungstätigkeit

----- Ende Optionale Angaben----

Erläuterungen zum Verarbeitungsverzeichnis

Nr. 1	Eindeutige Bezeichnung der dokumentierten Verarbeitung/ Verarbeitungstätigkeit auf Grundlage eines Fachprozesses. Es sollte eine in der Organisation geläufige Bezeichnung des Fachprozesses gewählt werden. Beispiele: - Allgemeine Kundenverwaltung - Customer-Relationship-Management (CRM)
Nr. 1	Nach der Unternehmensorganisation für die konkrete Verarbeitungstätigkeit verantwortlicher Fachbereich/verantwortliche Führungskraft (*sofern möglich und sinnvoll, zumindest als Funktionsbezeichnung*)
Nr. 2	Falls mehrere Verantwortliche gemeinsam für die Verarbeitungstätigkeiten verantwortlich sind, sind hier Name und Kontaktdaten des/der weiteren Verantwortlichen anzugeben (Firma/ladungsfähige Anschrift; Art. 30 Abs. 1 a) DSGVO, Art. 26 Abs. 1 DSGVO)
Nr. 3	Es ist zu bewerten, ob die Datenverarbeitung ein hohes Risiko für die Personen birgt, deren Daten verarbeitet werden. Ein hohes Risiko liegt u.a. dann vor, wenn sehr viele Personen von der Datenverarbeitung betroffen sind. Das gleiche gilt, wenn besonders schutzwürdige Daten (z.B. Gesundheitsdaten) umfangreich verarbeitet werden.
Nr. 4	Beispiele: - Verarbeitungstätigkeit: „Allgemeine Mitgliederverwaltung"; verfolgte Zweckbestimmungen: „Auftragsbearbeitung, Buchhaltung und Inkasso" - Verarbeitungstätigkeit: „Customer-Relationship-Management"; verfolgte Zweckbestimmungen: „Dokumentation und Verwaltung von Mitgliederbeziehungen, Marketing, Beschwerdemanagement, Kündigungsprozess" Eine Verarbeitungstätigkeit kann mehrere Teil-Geschäftsprozesse zusammenfassen. Dementsprechend kann eine Verarbeitung auch mehrere Zwecke umfassen, so dass auch mehrere Zweckbestimmungen angegeben werden können. Die erforderliche Detailtiefe hängt von der Tätigkeit des Verantwortlichen ab. Es können neben dem Fachprozess auch begleitende mitarbeiterbezogene Unterstützungsprozesse vorliegen wie z.B. zur Personalführung/-einsatzplanung. Diese können entweder als Teil einer anderen Verarbeitung oder als eigene Verarbeitung beschrieben sein.
Nr. 5	Die Nennung der einschlägigen Rechtsgrundlage ist für Rechenschaftspflichten und die Gewährleistung von Transparenzpflichten ggü. den betroffenen Personen notwendig. Die Rechtsgrundlage können z.B. eine gesetzliche Vorschrift oder eine Einwilligung durch den Betroffenen sein.
Nr. 6	Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, Art. 30 Abs. 1 c) DSGVO

Nr. 6.1	Als betroffene Personengruppen kommen beispielsweise Mitglieder, Arbeitnehmer, Schuldner usw. in Betracht.
Nr. 6.2	Den einzelnen Personengruppen sind die jeweils auf sie bezogenen verwendeten Daten oder Datenkategorien zuzuordnen. Damit sind keine personenbezogenen Daten, sondern "Datenbezeichnungen"/Datenkategorien gemeint (z.B. „Adresse“, „Geburtsdatum“, „Bankverbindung“). Werden solche Datenkategorien angegeben, so müssen diese so konkret wie möglich sein. Nicht ausreichend sind etwa Angaben wie „Mitgliederdaten“ oder Ähnliches. Beispiele: - Mitglieder: Adressdaten, Kontaktkoordinaten (einschl. Telefon-, Fax- und E-Mail-Daten), Geburtsdatum, Vertragsdaten, Bonitätsdaten, Betreuungsinformationen einschließlich Kundenentwicklung, Produkt- bzw. Vertragsinteresse, Statistikdaten, Abrechnungs- und Leistungsdaten, Bankverbindung - Beschäftigtendaten (Lohn und Gehalt): Kontaktdaten, Bankverbindung, Sozialversicherungsdaten, etc.
Nr. 7	Empfängerkategorien sind insbesondere am Prozess beteiligte weitere Stellen des Unternehmens oder andere Gruppen von Personen oder Stellen, die Daten – ggf. über Schnittstellen – erhalten z.B. in den Prozess eingebundene weitere Fachabteilungen, Vertragspartner, Mitglieder, Behörden, Versicherungen, Auftragsverarbeiter (z.B. Dienstleistungsrechenzentrum, Call-Center, Datenvernichter, Anwendungsentwicklung, Cloud Service Provider) usw.
Nr. 8	Drittländer sind solche außerhalb der EU/des EWR Beispiele für internationale Organisationen: Institutionen der UNO, der EU. Liegt keine der genannten Garantien vor, sind hier andere getroffene Garantien zu dokumentieren, Art. 49 Abs. 1. UAbs. 2 DSGVO.
Nr. 9	Anzugeben sind hier die konkreten Aufbewahrungs-/Löschfristen, die in Verarbeitungstätigkeiten implementiert sind, bezogen auf einzelne Verarbeitungsschritte, falls unterschiedlich. Soweit diese in einem Löschkonzept dokumentiert sind, reicht der Verweis auf das vorhandene und in der Verarbeitungstätigkeit umgesetzte Löschkonzept aus.
Nr. 10	Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO.
Nr. 10.1	Optional kann an dieser Stelle eine knappe Beschreibung der technischen Infrastruktur wie der technischen und organisatorischen Sicherheitsmaßnahmen angegeben werden, um ein besseres Verständnis der allgemeinen Beschreibung der technischen und organisatorischen Maßnahmen (siehe 10.2.) zu ermöglichen.
Nr. 10.2	Soweit sich die technischen und organisatorischen Maßnahmen schon aus vorhandenen Sicherheitsrichtlinien/Konzepten/Zertifizierungen ergeben, ist ein konkreter Verweis hierauf ausreichend. Insbesondere sind hier Abweichungen zu einem übergreifenden Sicher-

	heitskonzept (**siehe Hauptblatt Nr. 5**) zu dokumentieren. Wenn eine Datenschutz-Folgenabschätzung für die Verarbeitung hohe Risiken ausweist, so sind die zur Bewältigung dieser Risiken getroffenen Sicherheitsvorkehrungen für die Verarbeitung in der Datenschutz-Folgenabschätzung zu dokumentieren, Art. 35 Abs. 7 d) DSGVO. Ein Verweis auf das Vorhandensein einer Datenschutz-Folgenabschätzung ist eine sinnvolle optionale Angabe (siehe unten).
Optional	Im Hinblick auf die vielfältigen Nachweispflichten, denen die Organisation im Datenschutz unterliegt, kann es sinnvoll sein, weitere Aspekte zur Verarbeitungstätigkeit zu dokumentieren. Diese sind nur intern zu verwenden. Zu diesen zusätzlichen Dokumentationen, die sinnvollerweise hier erfolgen, gehören z. B. • *Angaben zur Zusammenstellung der Informationspflichten (insbes. Art. 13,14 DSGVO)* • *Verträge mit Dienstleistern (Art. 28 DSGVO)* • *Vereinbarungen zur gemeinsamen Verantwortung (Art. 26 DSGVO)* • *Eine Bewertung der Risiken der Verarbeitungstätigkeit für die Rechte und Freiheiten natürlicher Personen* • *durchgeführte Datenschutzfolgeabschätzungen zur Verarbeitungstätigkeit oder einzelnen Verarbeitungsschritten (Art. 35 DSGVO)*

Anlage 7

Technische und organisatorische Maßnahmen

1. Organisatorische Maßnahmen

☐ Ist ein betrieblicher Datenschutzbeauftragter bestellt?
☐ Nein
☐ Ja
Name: …….
Funktion: ……
E-Mail: ……
Telefon: ……..
☐ Mitarbeiter wurden nachweislich über Datenschutzrecht und Datensicherheit geschult.
☐ Alle Mitarbeiter sind nachweislich 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 ____).

2. Vertraulichkeit

a) <u>Zutritts-, Zugangs-, Speicher- und Datenträgerkontrolle</u>
Maßnahmen, die geeignet sind, Unbefugten den Zugang zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet werden.

☐ Schriftliche Zutrittsregelungen zum Betreten des Rechenzentrums/der Räume mit DV-Anlagen sind vorhanden
☐ Alarmanlage
☐ Automatisches Zutrittskontrollsystem, Ausweisleser
☐ Türsicherung (elektrischer Türöffner, Zahlenschloss usw.)
☐ Schlüsselregelung (Schlüsselverwaltung: Schlüsselausgabe etc.)
☐ Sicherheitsschlösser
☐ Chipkarten-/Transponder-Schließsystem
☐ Biometrie (Fingerabdrücke o. ä.)
☐ Manuelles Schließsystem
☐ Schranken/Vereinzelungsanlagen (Drehkreuze o. ä.)
☐ Magnetschleusen
☐ Werkschutz/Pförtner
☐ Empfang mit Anmeldung
☐ Sorgfältige Auswahl von Wachpersonal

- ☐ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Lichtschranke/Bewegungsmelder
- ☐ Feuerfeste Türen
- ☐ Absicherung von Gebäudeschächten
- ☐ Fenstervergitterung
- ☐ Panzerglas
- ☐ Videoüberwachung der Zugänge

b) <u>Zugangs- und Benutzerkontrolle</u>

Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- ☐ Passwortvergabe
  Länge des Passworts: … Zeichen
  Wechselfristen … Wochen/Monate
  Anzahl der Fehleingaben …
- ☐ Chipkarte mit PIN/Passwort
- ☐ Authentifikation mit Benutzername/Passwort
- ☐ Biometrisches Merkmal mit PIN/Passwort
- ☐ Einsatz von VPN-Technologie
- ☐ Verschlüsselung von Smartphone-Inhalten
- ☐ Verschlüsselung von mobilen Datenträgern

c) <u>Zugriffskontrolle</u>

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.

- ☐ Schriftliches Berechtigungskonzept vorhanden
- ☐ Zuordnung von Benutzerrechten/Erstellen von Benutzerprofilen
- ☐ Verwaltung der Rechte durch System-Administrator
- ☐ Anzahl der Administratoren auf das "Notwendigste" reduziert
- ☐ Gesicherte Nutzung von USB-Schnittstellen
- ☐ Automatische Sperrung des Arbeitsplatzes
- ☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
  - ☐ Die Protokolle werden ausgewertet, zeitlicher Abstand: ….
- ☐ Einsatz von Akten-/Datenträgervernichtern bzw. Dienstleistern unter Beachtung von DIN 66399
- ☐ Verschlüsselung von Datenträgern
- ☐ Sichere Aufbewahrung von Datenträgern
- ☐ Ordnungsgemäße Vernichtung von Datenträgern
- ☐ Löschungskonzept für Daten
- ☐ Protokollierung der Vernichtung

d) <u>Transport- und Übertragungskontrolle</u>

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen *Übertragung 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.*

- ☐ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☐ Firewall: Die nach dem Stand der Technik erforderlichen Firewall-Technologien sind implementiert und werden auf dem aktuellen Stand gehalten
- ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form bzw. Verschlüsselung
- ☐ E-Mail-Verschlüsselung
- ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☐ Protokollierung von Übermittlungen
- ☐ Erstellen einer Übersicht von Datenträgern, Aus- und Eingang
- ☐ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und Fahrzeugen
- ☐ Sicherung von Datenträgertransporten (verschließbarer Transportbehälter), auch für Papier

e) <u>Auftragskontrolle</u>

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

- ☐ Vorhandene Vereinbarungen zur Auftragsverarbeitung
- ☐ Kontrolle der Vertragsausführung
- ☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☐ Regelung zu Wartungen (speziell Fernwartung)

3. Integrität

a) Eingabekontrolle/Verarbeitungskontrolle

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

- ☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- ☐ Protokollauswertungsroutinen/-systeme vorhanden
- ☐ Aufbewahrungs-/Löschungsfrist für Protokolle vorhanden

b) <u>Dokumentationskontrolle</u>
Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.

- ☐ Führung eines Verarbeitungsverzeichnisses
- ☐ Dokumentation der eingesetzten IT- Systeme und deren Systemkonfiguration
- ☐ Zulässigkeit eines Datentransfers in Drittländer ist gegeben

4. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und im Störfall wieder hergestellt werden können.

- ☐ Unterbrechungsfreie Stromversorgung (USV)
- ☐ Überspannungsschutz
- ☐ Schutz gegen Umwelteinflüsse (Sturm, Wasser)
- ☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☐ Feuer- und Rauchmeldeanlagen
- ☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☐ Testen von Datenwiederherstellung
- ☐ Klimaanlage in Serverräumen
- ☐ Schutzsteckdosenleisten in Serverräumen
- ☐ Feuerlöschgeräte in Serverräumen
- ☐ Backups (Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und -ort)
- ☐ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☐ Virenschutzsystem
- ☐ Spiegelung von Festplatten (z. B. RAID-Verfahren)
- ☐ Konzept für Katastrophenfall vorhanden

5. Trennungsgebot

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

- ☐ Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern
- ☐ Logische Mandantentrennung (softwareseitig)
- ☐ Trennung von Produktiv- und Testsystem
- ☐ Festlegung Technologie von Datenbankrechten
- ☐ Trennung von Daten verschiedener Auftraggeber

Anlage 8

Der behördliche Datenschutzbeauftragte (DSB)

MUSTER

Benennung eines/r behördlichen Datenschutzbeauftragten

Herrn/Frau
Michael(a) Muster
Mustergasse 1
33333 Musterstadt

Sehr geehrte/r Frau/Herr _____,

ich/wir benennen Sie mit sofortiger Wirkung zur/m Datenschutzbeauftragten gemäß Artikel 37 Abs. 1 a) EU-Datenschutzgrundverordnung (DSGVO) in Verbindung mit § _____ Landesdatenschutzgesetz. In Ihrer Funktion als Datenschutzbeauftragte/r sind Sie der Geschäftsführung unmittelbar unterstellt.

Zuständiges Mitglied der Geschäftsführung ist

_____

Ihre Aufgaben als Datenschutzbeauftragte/r ergeben sich aus den Artikeln 37 bis 39 DSGVO sowie § _____Landesdatenschutzgesetz. In Anwendung Ihrer Fachkunde auf dem Gebiet des Datenschutzes sind Sie weisungsfrei. Bei der Erfüllung Ihrer Aufgaben sind Sie an die Wahrung der Geheimhaltung und der Vertraulichkeit gebunden. Über Ihre Tätigkeit werden Sie der Geschäftsführung laufend Bericht erstatten.

Erforderliche Organisationsanweisungen schlagen Sie der Geschäftsführung vor.

Die Stellung des behördlichen Datenschutzbeauftragten ist in § ___ Landesdatenschutzgesetz geregelt.

_____ _____
Ort, Datum Unterschrift Hauptgeschäftsführer

Mit der Benennung bin ich einverstanden

_____
Unterschrift, Datenschutzbeauftragte/r

Anlage 9

Auftragsverarbeitung – Hinweise für Handwerksorganisationen

Musterformulierungen

1. Gegenstand und Dauer des Auftrags

➔ Der Gegenstand und die Dauer des Auftrags müssen individuell mit dem Auftragsverarbeiter verhandelt und festgelegt werden.

➔ Musterformulierungen sind wegen der Individualität der Vereinbarungen nicht möglich.

2. Umfang, Art und Zweck der Datenverarbeitung

Formulierungsvorschlag:

„Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im sachlichen und zeitlichen Rahmen dieses Auftrages sowie nach Weisung des Auftraggebers. Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

Die Verarbeitung der Daten auch durch Unterauftragnehmer findet

☐ ausschließlich im Gebiet der Bundesrepublik Deutschland,

☐ in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum,

☐ in einem Drittstaat (Nennung des Drittstaats _____)

statt. In letzterem Fall weist der Auftragnehmer für die Rechtmäßigkeit entsprechende vertragliche oder sonstige, der DSGVO entsprechenden Rechtsgrundlagen nach.“

3. Technische und organisatorische Maßnahmen

Formulierungsvorschlag:

„Der Auftragnehmer wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den gesetzlichen Anforderungen genügen. Hierbei sind die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen. Die technisch-organisatorischen Maßnahmen des Auftragnehmers sind gesondert zu diesem Vertrag festzulegen und sind Bestandteil des Vertrags.

Der Auftragnehmer gewährleistet ein Verfahren zur Überprüfung der technischen und organisatorischen Maßnahmen. Er ist verpflichtet, die technischen und organisatorischen Maßnahmen an den Stand der Technik anzupassen, soweit dies erforderlich und wirtschaftlich zumutbar ist. Der Auftraggeber ist über wesentliche Änderungen vorab zu informieren. Die Änderungen sind schriftlich niederzulegen und werden Vertragsbestandteil. Vorschläge des Auftraggebers für Änderungen hat der Auftragnehmer zu prüfen. Der Auftraggeber ist über das Ergebnis zu informieren.

Beauftragt der Auftragnehmer zur Erfüllung seiner vertraglichen Pflichten einen Unterauftragnehmer, stellt er sicher, dass die erforderlichen technischen und organisatorischen Maßnahmen vom Unterauftragnehmer getroffen werden und dem Stand der Technik entsprechen."

4. Berichtigung, Sperrung und Löschung von Daten, Auskunft über Daten

Formulierungsvorschlag:

„Der Auftragnehmer hat die Daten nach Weisung des Auftraggebers zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung, Sperrung oder Löschung seiner Daten wendet, leitet der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiter. Das gleiche gilt für Auskunftsersuche."

5. Kontrollen und sonstige Pflichten des Auftragnehmers

Formulierungsvorschlag:

„Der Auftragnehmer ist verpflichtet, das Datengeheimnis sowie etwaige berufliche Verschwiegenheitsverpflichtungen zu wahren. Er hat bei der Verarbeitung ausschließlich Beschäftigte einzusetzen, die entsprechend verpflichtet und geschult sind. Er hat insbesondere sicherzustellen, dass alle Personen, die von ihm mit der Bearbeitung oder Erfüllung dieses Vertrages betraut sind, sorgfältig ausgewählt werden, die gesetzlichen Datenschutzbestimmungen beachten und die vom Auftraggeber erlangten Informationen nicht unbefugt an Dritte weitergeben oder anderweitig verwerten.

Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für sämtliche vertragsrelevanten Angelegenheiten des Datenschutzes. Der Auftragnehmer hat Frau/Herrn_____ als betrieblichen Datenschutzbeauftragten bestellt.

Der Auftragnehmer ist verpflichtet, ein Verarbeitungsverzeichnis gemäß Art. 30 Abs. 2 DSGVO zu führen. Der Auftragnehmer gewährt dem Landesdatenschutzbeauftragten Zugang zu den Arbeitsräumen und unterwirft sich der Kontrolle nach Maßgabe des Landesdatenschutzgesetzes in seiner jeweiligen Fassung. Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontroll- und Ermittlungshandlungen der Aufsichtsbehörde."

6. Unterauftragsverhältnisse

Formulierungsvorschlag:

„Der Auftraggeber genehmigt die gesondert aufgelisteten Unterauftragsverhältnisse, die der Auftragnehmer vor Abschluss dieser Vereinbarung begründet hat. Über Änderungen hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Abschluss neuer Unterauftragsverhältnisse bedarf der vorherigen Zustimmung des Auftraggebers.

Der Auftragnehmer hat dem Unterauftragnehmer dieselben Pflichten aufzuerlegen, die er selbst gegenüber dem Auftraggeber zu erfüllen hat. Der Unterauftragnehmer ist sorgfältig auszuwählen. Der Auftragnehmer haftet gegenüber dem Auftraggeber vollumfänglich für Datenverstöße seiner Unterauftragnehmer."

7. Kontrollrechte des Auftraggebers

Formulierungsvorschlag:

„Der Auftraggeber hat das Recht, vor Beginn und während der Datenverarbeitung die Einhaltung der vom Auftragnehmer sowie von den Unterauftragnehmern getroffenen technischen und organisatorischen Maßnahmen zu kontrollieren oder von zu benennenden Prüfern kontrollieren zu lassen. Das Ergebnis ist zu dokumentieren.

Der Auftragnehmer gewährleistet die Möglichkeit zur Kontrolle. Hierzu weist er dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO nach. Der Nachweis kann durch Vorlage aktueller Testats oder durch Berichte unabhängiger Prüfer (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, Datenschutzauditoren, Qualitätsauditoren) erbracht werden.

Haben sich der Auftragnehmer und die von ihm beauftragten Unterauftragnehmer Verhaltensregeln unterworfen oder ein Zertifizierungsverfahren erfolgreich durchlaufen, sind sie verpflichtet, dem Auftraggeber dies nachzuweisen. Zertifikate sind zu aktualisieren.

Der Auftraggeber ist berechtigt, Stichprobenkontrollen durchzuführen. Diese sind anzukündigen. Würde die Ankündigung den Zweck der Prüfung gefährden oder besteht ein dringender Anlass zur Kontrolle, ist eine Ankündigung entbehrlich."

8. Mitteilung bei Verstößen

Formulierungsvorschlag:

„Der Auftragnehmer meldet dem Auftraggeber unverzüglich sämtliche Verstöße gegen Pflichten aus diesem Vertrag. Dies gilt insbesondere bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen von Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung bzw. zum Ausschluss möglicher nachteiliger Folgen für die Betroffenen zu ergreifen."

9. Weisungsbefugnis des Auftraggebers

Formulierungsvorschlag:

„Der Auftraggeber ist berechtigt, dem Auftragnehmer jederzeit Weisungen zu erteilen, insbesondere hinsichtlich der Art, des Umfangs und des Zeitpunkts der Verarbeitung von Daten. Die Weisungen des Auftraggebers erfolgen in Textform.

Erachtet der Auftragnehmer eine Weisung des Auftraggebers als rechtswidrig, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Er ist berechtigt, die Durchführung der Weisung auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

Erteilt der Auftraggeber Einzelweisungen bzgl. des Umgangs mit personenbezogenen Daten, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, z.B. Änderungen der technischen und organisatorischen Maßnahmen, werden sie als Antrag auf Leistungsänderung behandelt.“

10. Löschung von Daten und Rückgabe von Datenträgern

„Der Auftragnehmer hat dem Auftraggeber sämtliche in seinen Besitz befindlichen personenbezogenen Daten, erstellte Verarbeitungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, unverzüglich nach Erfüllung des Vertrags oder nach Aufforderung durch den Auftraggeber, spätestens mit Beendigung der Zusammenarbeit auszuhändigen oder nach vorheriger Zustimmung des Auftraggebers datenschutzgerecht zu vernichten. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Ein Zurückbehaltungsrecht ist ausgeschlossen.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind vom Auftragnehmer entsprechend der geltenden Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.“