Referat Recht

Verteiler:
Konferenz der Verbände
Vorstand des GdW
Präsidium des Verbandsrates
Alle GdW-Fachausschüsse

06.02.2018 He/Neu/Mey
Telefon: +49 30 82403-141
E-Mail: herlitz@gdw.de

Das Wichtigste:

Am 25. Mai 2018 tritt die neue Datenschutzgrundverordnung in Kraft. Der GdW hat hierzu einen Workshop mit Experten durchgeführt. Die wesentlichen Ergebnisse sind, dass mit der neuen Datenschutzgrundverordnung vor allem Regelungen im Hinblick auf den Umgang mit Daten, Informationspflichten und neue Anforderungen an die Dokumentation zu beachten sind. Insofern gilt es vor allem, die internen Prozesse zu optimieren und auf das neue Datenschutzrecht anzupassen, vgl. hierzu auch GdW-Rundschreiben vom 23. Juni 2017.

Anderes als bisher gilt, dass Datenschutz zukünftig "Chefsache" ist und höhere Bußgelder verhängt werden können als nach dem bisherigem Datenschutzrecht.

Als erstes sind daher zunächst folgende Schritte erforderlich:

- Bestellung eines Datenschutzbeauftragten und eines Vertreters sowie bei externen Datenschutzbeauftragten eines internen Ansprechpartners,
- Erarbeitung eines Verzeichnisses der Verarbeitungstätigkeiten,
- Erstellung und Bereitstellung von Informationshinweisen zur Datenerhebung,
- Mitarbeiterschulung
- Anpassung der Verträge mit Unternehmen, die in Ihrem Auftrag Daten verarbeiten (Auftragsverarbeiter)
- Anpassung der Verpflichtung auf Datengeheimnis
- Überprüfung und Anpassung der Webseite (Datenschutzerklärung, Impressum)
- Erstellung von notwendigen Dokumentationen, wie z. B.: IT-Infrastrukturübersicht, Backupkonzept, Notfallplan, Passwortrichtlinie und Umgang mit Passwörtern, Archivierungs- bzw. Löschkonzept, Richtlinien und Arbeitsanweisungen etc. und die Vornahme der entsprechenden technischen und organisatorischen Maßnahmen (TOMs)

Der GdW wird auf der Grundlage der Ergebnisse des Workshops eine umfassende Handlungsempfehlung herausgeben.

Datenschutzgrundverordnung – Informationen über erste Ergebnisse aus dem GdW-Workshop

Sehr geehrte Damen und Herren,

am 25. Mai 2018 tritt die neue Datenschutzgrundverordnung in Kraft. Im Vergleich zu anderen europäischen Ländern ist das deutsche Datenschutzrecht bereits umfassend normiert. Die europäische Datenschutzgrundverordnung bedeutet daher vor allem neue Anforderungen an den Umgang mit Daten. Darauf folgen verstärkte Informationspflichten, detailliertere Dokumentationspflichten über Datenerhebung, -verarbeitung und -löschung sowie insgesamt eine Anpassung vor allem interner Prozessabläufe.

Der GdW hat hierzu am 16. Januar 2018 einen Workshop durchgeführt, deren wesentliche Ergebnisse nachfolgend dargestellt werden sollen. Hiervon unabhängig werden die Ergebnisse in einer ersten Handlungsempfehlung für die Wohnungsunternehmen dargestellt. Die in diesem Schreiben beigefügten Muster werden die für diese Handlungsempfehlung ggf. aktualisiert. Sie sollen also eine erste Orientierung darstellen.

Die wesentlichen Ergebnisse des Workshops:

I.
Allgemeine Anmerkungen

Die Anforderungen der Verordnung (EU) 2016/679 (DSGVO) gelten unmittelbar ab dem 25. Mai 2018. Die neue Datenschutzgrundverordnung sieht keine allgemeine Bestandschutzregelung für eine bereits laufende Datenverarbeitung vor. Insofern ist die Datenverarbeitung in sämtlichen Mietverhältnissen ebenso wie die allgemeine Datenverarbeitung von Wohnungsunternehmen bis zu diesem Zeitpunkt an die Anforderungen der Verordnung anzupassen.

Trotz der Vielzahl neuer Anforderungen bleibt Spielraum für einen produktiven und erfolgversprechenden Anpassungsprozess. Neben ersten Schulungen bzw. Sensibilisierungsmaßnahmen aller mit der Datenverarbeitung befassten Mitarbeiter sollte die Anlegung eines Verzeichnisses der Verarbeitungstätigkeit nach Art. 30 DSGVO im Mittelpunkt stehen. Mit diesem Verzeichnis der Verarbeitungstätigkeiten erfolgt zwangsläufig eine umfassende Bestandsaufnahme und -analyse sämtlicher Datenverarbeitungstätigkeiten im Unternehmen. Eine erste Orientierung für ein Verarbeitungsverzeichnis ist als **Anlage 1** beigefügt.

II.
Der Vermieter als Verantwortlicher

Die Datenschutzgrundverordnung richtet sich an Wohnungsunternehmen und ist "Chefsache". Der Vorstand oder der Geschäftsführer, soweit er über die Zwecke und Mittel der Verarbeitung der personenbezogener Daten (mit)entscheidet, ist "Verantwortlicher", vgl. Art. 4 Abs. 7 DSGVO.

Wesentlich für den Verantwortlichen ist, dass ihn eine konkrete Organisationsverantwortung trifft, die weit über die Gewährleistung der materiellen Rechtmäßigkeit der Datenverarbeitung hinausgeht.

Um dem Grundsatz der Rechenschaftspflicht gerecht zu werden, ist eine umfassende Bestandsaufnahme aller – auch "analoger Tätigkeiten" mit Bezug zu personenbezogenen Daten, deren Analyse und risikobezogene Bewertung sowie deren dokumentierte Neuorganisation mit dem Ziel der Einhaltung der materiellen Anforderungen der DSGVO erforderlich.

Diese Organisationsverantwortung bezieht sich insbesondere auf die strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geführt wird. Erfasst sind damit planmäßige Zusammenstellungen und die Erhebung der Daten, die aufgrund eines formalen Ordnungsschemas erhoben werden.

- Der Verantwortliche hat zum 25. Mai 2018 organisatorische Vorkehrungen zu treffen, die Gewähr dafür bieten, dass sein Unternehmen im Fall einer Datenschutzverletzung datenschutzkonform handeln könnte.

III.
Benennung eines Datenschutzbeauftragten und stellv. Datenschutzbeauftragten

Innerhalb der Konzeption der DSGVO bedeutet die Organisationsverantwortlichkeit auch die Bestellung eines (internen oder externen) Datenschutzbeauftragten und eines stellvertretenden Datenschutzbeauftragten. Dem Datenschutzbeauftragten kommen echte Kontroll- und Überwachungsaufgaben zu.

Danach obliegen dem Datenschutzbeauftragten u. a. gemäß Art. 39 DSGVO folgende Aufgaben:

- Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach der DSGVO;

- Überwachung der Einhaltung der DSGVO sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten;

- Zusammenarbeit mit der Aufsichtsbehörde;

- Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation und ggf. Beratung zu allen sonstigen Fragen.

Hinweis: Nennen Sie den Datenschutzbeauftragten und seinen Stellvertreter auf der Homepage Ihres Unternehmens und teilen Sie den bestellten Datenschutzbeauftragen der für Sie zuständigen Datenschutzbehörde (je Bundesland) mit.

Eine Benennung ist in folgenden Fällen erforderlich:

- es werden in der Regel mindestens **zehn Personen** ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt **oder**

- es werden Verarbeitungen vorgenommen, die einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO (DS-Folgenabschätzung) unterliegen oder es werden personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet;

In den letzteren Fällen muss unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen ein DSB benannt werden.

Für den Datenschutzbeauftragten bestehen durch die DSGVO deutlich mehr Pflichten, die damit einhergehend auch das Risiko für eine Pflichtverletzung steigern. Das birgt für Unternehmen die Gefahr, den wesentlich höheren Bußgeldern der DSGVO ausgesetzt zu sein. Dies kann sich durch die Rückgriffsmöglichkeit des Unternehmens letztlich auch auf die Haftung des Datenschutzbeauftragten auswirken. Auf den Abschluss entsprechender Versicherungen wird hingewiesen.

IV.
Verzeichnis von Verarbeitungstätigkeiten ("Verarbeitungsverzeichnis")

Die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten folgt aus der Pflicht, die Einhaltung der DSGVO nachweisen zu können. **Das Verarbeitungsverzeichnis ist Dreh – und Angelpunkt der Verordnung, gewissermaßen der "Spielmacher" des neuen Datenschutzrechts.** Die Führung eines Verzeichnisses von Verarbeitungstätigkeiten obliegt dem Verantwortlichen.

Das aus dem Bundesdatenschutzgesetz bekannte Verfahrensverzeichnis (vgl. § 4 g Abs. 2 und Abs. 2 a BDSG; dort "Übersicht" genannt) wird durch das sog. Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO abgelöst. Dieses Verzeichnis betrifft sämtliche – auch teilweise – automatisierte Verarbeitungen sowie nicht automatisierte Verarbeitungen personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. In der Praxis wird wegen der Unterschiede bei den eingesetzten Verfahren das Verarbeitungsverzeichnis aus einer Reihe von Einzelbeiträgen bestehen müssen. Das Verfahrensverzeichnis wird somit die Summe der einzelnen Verfahrensbeschreibungen sein. Das Verzeichnis der Verantwortlichen muss nach Art. 30 Abs. 1 DSGVO wesentliche Angaben zur Verarbeitung beinhalten wie zum Beispiel die Zwecke der Verarbeitung und eine Beschreibung der Kategorien der personenbezogenen Daten, der betroffenen Personen und der Empfänger.

Mit der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten sind keinesfalls alle von der Datenschutzgrundverordnung geforderten Dokumentationspflichten erfüllt. So müssen beispielsweise auch das Vorhandensein von Einwilligungen (Art. 7 Abs. 1 DGSVO), die Ordnungsmäßigkeit der gesamten Verarbeitung (Art. 24 Abs. 1 DGSVO) und das Ergebnis von Datenschutz-Folgenabschätzungen (Art. 35 Abs. 7 DGSVO) durch entsprechende Dokumentationen nachgewiesen werden. Gegebenenfalls können diese Rechenschaftspflichten dem Verarbeitungsverzeichnis beigefügt werden bzw. in das Verarbeitungsverzeichnis integriert werden. Ein

Muster für ein Verarbeitungsverzeichnis wurde von der Datenschutzkonferenz für 2017 angekündigt, nach unserer Kenntnis bislang jedoch nicht veröffentlicht.

Das Verzeichnis, welches wir Ihnen als Entwurf als **Anlage 1** und erste Orientierung überreicht haben, sollte folgende Angaben enthalten:

- den Namen und die Kontaktdaten des Wohnungsunternehmens sowie eines etwaigen Datenschutzbeauftragten (und ggf. des Stellvertreters);
- die Zwecke der Verarbeitung;
- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern
- oder internationalen Organisationen;
- die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
- eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Sicherheit der Verarbeitung).

Auf Anfrage ist das Verzeichnis der Aufsichtsbehörde zur Verfügung zu stellen.

Es wird darauf hingewiesen, dass der Stand des Musters und des in Ihrem Unternehmen angewendeten Verarbeitungsverzeichnis fortwährend zu optimieren ist. Die GDD (Gesellschaft für Datenschutz und Datensicherheit e.V.) hat ebenfalls ein Muster für Verarbeitungstätigkeiten veröffentlicht, welches unter https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_5.pdf/view abgerufen werden kann.

V.
Der Ausbau der Betroffenenrechte

Die neue Datenschutzgrundverordnung bietet bei Datenverarbeitungen „zur Wahrnehmung berechtigter Interessen“ Spielraum für eine Vielzahl datenbezogener Geschäftsmodelle. Im Gegenzug erweitert bzw. präzisiert die Datenschutzgrundverordnung für alle Datenverarbeitungen die Rechte der Betroffenen. Es gelten erweiterte Transparenzvorschriften. Wohnungsunternehmen müssen betroffene Personen also deutlich umfassender als bislang und in einer nachvollziehbaren Weise darüber informieren, ob und wie sie deren Daten verarbeiten. Macht eine betroffene Person ihr Auskunftsrecht darüber geltend, ob und welche personenbezogenen Daten ein Wohnungsunternehmen von ihr verarbeitet, muss ihr das Wohnungsunternehmen als Verantwortliche u. a. eine Kopie der verarbeiteten personenbezogenen Daten in einer für sie nutzbaren/lesbaren Form zur Verfügung stellen.

Auch die Melde- und Benachrichtigungspflichten gegenüber den betroffenen Personen und die in diesem Zusammenhang getroffene Definition einer Datenschutzverletzung wurden deutlich erweitert. Grundsätzlich muss das verantwortliche Unternehmen der Aufsichtsbehörde jede Datenschutzverletzung unverzüglich, d. h. möglichst innerhalb von 72 Stunden melden, nachdem dem Verantwortlichen die Verletzung bekannt wurde. Nur ausnahmsweise besteht keine Pflicht zur Meldung bei der Aufsichtsbehörde, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten der von der Datenschutzverletzung betroffenen Personen führt. Aber auch diese Prüfung ist mit dem Ergebnis zu dokumentieren.

Zudem muss der Verantwortliche grundsätzlich die betroffenen Personen selbst ohne unangemessene Verzögerung benachrichtigen, wenn eine Datenschutzverletzung voraussichtlich ein hohes Risiko für ihre persönlichen Rechte und Freiheiten zur Folge hat.

Im Überblick:

- Informationspflichten Art. 13 und 14 DSGVO
- Auskunftsrecht, Recht auf Kopie Art. 15 DSGVO
- Recht auf unverzügliche Berichtigung Art. 16 DSGVO
- Recht auf unverzügliche Löschung und Benachrichtigung von (Weiter-)Verarbeitern Art. 17 Abs. 1 und 2 DSGVO, „Recht auf Vergessenwerden", Art. 19 DSGVO
- Recht auf Einschränkung der Verarbeitung Art. 18 DSGVO
- Recht auf Datenübertragbarkeit bei einwilligungsbezogener oder vertraglich legitimierter Datenverarbeitung in automatisierten Verfahren, Art. 20 DSGVO
- Widerspruchsrecht bei Datenverarbeitung zur Wahrnehmung von Aufgaben im öffentlichen Interesse oder zur Wahrnehmung berechtigter Interessen des Verantwortlichen, Art. 21 DSGVO
- Schutzrechte bei Profiling im Rahmen einwilligungsbasierter oder vertraglich legitimierter automatisierter Entscheidungen bzw. Profiling-Maßnahmen, Art. 22 Abs. 2 DSGVO
- Benachrichtigung über Datenschutzverletzungen, Art. 34 DSGVO

VI.
Objektive Pflichten von Verantwortlichen und Auftragsverarbeitern

Zugleich werden technisch-organisatorische Maßnahmen stärker als bisher differenziert und unterliegen nunmehr auch explizit Überwachungs- und Aktualisierungspflichten (Art. 24 Abs. 1 Satz 2 DSGVO):

- Art. 12 DSGVO: Verpflichtung zur transparenten Information
- Art. 25 DSGVO: datenschutzfreundliche Voreinstellungen, z.B. Datenminimierung
- Art. 28 DSGVO: erweiterte Festlegungen im Auftragsverarbeitungsvertrag zu technisch-organisatorischen Maßnahmen

- Art. 30 DSGVO: Verzeichnis von Verarbeitungstätigkeiten: gegenüber §§ 4g Abs. 2, 4e Satz 1 BDSG a.F. in Umfang und Tiefe erweiterte Verarbeitungsdokumentation
- Art 33 DSGVO: Meldung von Datenschutzverletzungen an die Aufsichtsbehörde (ohne Begrenzungen des § 42a BDSG a.F.)
- Art 35 DSGVO: Datenschutzfolgenabschätzung zur strukturierten Bewertung und Datenschutzoptimierung von Verarbeitungen mit hohem Risiko für Rechte und Freiheiten der betroffenen Personen ("Datenschutz-UVP") ggf. mit anschließendem Konsultationsverfahren (Art. 36 DSGVO, weiter als § 4d BDSG a.F.).

Als **Anlage 2** ist ein Entwurf eines Mietinteressentenbogens sowie ein entsprechendes Informationsblatt als **Anlage 3** beigefügt. Auch diese werden wir aktualisieren und Ihnen mit der Handlungsempfehlung als vorläufige Endfassung überreichen. Insofern dienen auch diese Muster als Orientierung, die Sie ggf. bereits jetzt mit Ihrer zuständigen Aufsichtsbehörde abstimmen können.

VII.
Pflichten der Arbeitsgeber

Die oben benannten Grundsätze gelten auch für Arbeitgeber im Verhältnis zu Mitarbeitern und Angestellten. Darüber hinaus gilt § 26 BDSG 2018, der im Wesentlichen dem § 32 BDSG a.F. entspricht.

Folgende Punkte sind im Kern zu beachten:

- Information der Mitarbeiter über die neuen gesetzlichen Regelungen.
- Überprüfung der Personalakten auf wesentliche Grundsätze wie dem berechtigten Interesse der Datenerhebung, dem Grundsatz der Datenminimierung oder der Löschung von Daten.
- Überprüfung der Aufbewahrungsfristen für die Erstellung eines Löschkonzeptes.

VIII. Höhere Bußgelder – erweiterte Haftung

Art. 83 DSGVO sieht für Unternehmen Bußgelder von bis zu 4 % des globalen Umsatzes vor. An Verstößen gegen die DSGVO beteiligte natürliche Personen müssen mit Geldbußen von bis zu 20 Mio. EUR rechnen. Damit verschärft sich der Bußgeldrahmen gegenüber dem bisherigen Recht drastisch. Bislang sah § 43 BDSG Bußgelder von maximal 300.000 EUR vor.

Nach Art. 82 Abs. 1 DSGVO sind materielle und – als Neuerung auch ausdrücklich – immaterielle Schäden zu erstatten, die auf Verstößen gegen die Verordnung beruhen. Eine weitere Neuerung ist die ausdrückliche Erweiterung der Haftung auch auf Auftragsverarbeiter.

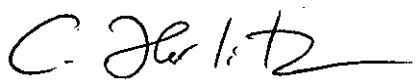
Weitere Themen wie der Umgang mit Social Media, der Überprüfung der Vertragsbeziehungen mit Auftragsverarbeitern, Haftungsfragen und nicht zuletzt Empfehlungen im Bereich der IT-Dienstleister werden wir in der Handlungsempfehlung zum Datenschutz, die im Wesentlichen von den Experten des Workshops erstellt wird, überreichen und erörtern.

Anlagen:

- Anlage 1 – Verfahrensverzeichnis
- Anlage 2 – Fragebogen für Mietinteressenten
- Anlage 3 – Informationsblatt Mietinteressenten
- Anlage 4 – SCHUFA-Hinweis zu Mietanträgen
- Anlage 5 – SCHUFA-Information
- Anlage 6 – Verpflichtung auf die Vertraulichkeit

Sämtliche Anlagen dienen als erste Orientierung und sollten auf die Besonderheiten in Ihrem Unternehmen angepasst und ggf. mit Ihrer Aufsichtsbehörde abgestimmt werden.

Mit freundlichen Grüßen



Carsten Herlitz
Justiziar