sikker
Datenschutz & Compliance

Ausgewählte Aspekte des Datenschutzes (DS-GVO)

Immobilienunternehmen

sikker
Datenschutz & Compliance

Allgemeine Gleichbehandlung gemäß AGG

Wir halten uns selbstverständlich an das geltende Gesetz zur Allgemeinen Gleichbehandlung (AGG). Die Texte in dieser Präsentation liegen größtenteils in der männlichen Form der Ansprache vor. Dies dient ausschließlich der besseren Lesbarkeit und ist frei von jeglicher Form der Ungleichstellung.

Selbstredend richten sich die Ausführungen sowohl an Damen, Herren und Intersexuelle Menschen.

sikker
Datenschutz & Compliance

Verarbeitungs-grundlagen

Vorschriften, die eine Datennutzung erlauben, finden sich im Wesentlichen in Art. 6 der DS-GVO. Diese Regelungen werden durch die §§ 22, 24, 26 des BDSG ergänzt. Bspw.:

- die betroffene Person hat ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- die Verarbeitung ist für die **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung **vorvertraglicher Maßnahmen** erforderlich, die auf Antrag der betroffenen Person erfolgen;
- die Verarbeitung ist zur **Wahrung der berechtigten Interessen des Verantwortlichen** oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt;
- die Verarbeitung ist erforderlich zur Begründung, Durchführung oder Beendigung eines **Beschäftigungsverhältnisses.**

sikker
Datenschutz & Compliance

Eine Einwilligungserklärung ist stets freiwillig!

- Aufklärung zur Datennutzung in einfacher, klarer und verständlicher Sprache
- Angaben zu Daten und Zweck der Datenverarbeitung
- Widerrufsmöglichkeit für die Zukunft (der Widerruf muss so einfach möglich sein, wie die Erteilung der Einwilligung)
- der Verantwortliche der Datenverarbeitung muss erkennbar sein
- die Einwilligungserklärung ist hervorzuheben, wenn diese zusammen mit anderen Informationen oder Erklärungen erfolgt (z.B. AGB)

NEU Einwilligungen müssen nicht mehr schriftlich erfolgen, jedoch ist unbedingt die Nachweisführung zu beachten (das Beweislastrisiko liegt beim Unternehmen)

- **PRÜFUNG der bestehenden Einwilligungserklärungen** auf Rechtskonformität → Fortgeltung
- **AUSTAUSCH der bestehenden Einwilligungserklärungen** ohne Rechtskonformität (Elektronisch und in Papierdokumenten)
- **IT-ANFORDERUNGEN für Dokumentation** der Einwilligungserklärungen
- **REVISIONSSICHERHEIT**
  Möglichkeit für (Teil-) Widerruf, Löschung, Änderung
  Abbildung der Historie
  Beweisverwertbarkeit
  Visualisierung für Auskunftsrechte etc.

Informationspflichten bei Datenerhebung

Bei Direkterhebung sind die folgenden Informationen gem. Art. 13 Abs. 1 DS-GVO zum Zeitpunkt der Erhebung bereitzustellen:

- Name und Kontaktdaten des Verantwortlichen, ggf. des Vertreters;
- Kontaktdaten des DSB (bei Bestellpflicht des Unternehmens);
- **Zweck** und **Rechtsgrundlage** der Datenverarbeitung;
- berechtigte Interessen des Verantwortlichen oder eines Dritten;
- ggf. die Empfänger oder **Kategorien von Empfängern** von personenbezogenen Daten;
- ggf. die Datenübermittlung in ein Drittland;
- die **Speicherdauer** für personenbezogene Daten;
- Informationen zu **Betroffenenrechten** auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung sowie das Recht auf Widerspruch zur Datennutzung sowie des Rechts auf Datenübertragbarkeit;

- Information zum Recht auf **Widerruf** bei Datenverarbeitung auf Grund einer Einwilligung;
- das Bestehen des **Beschwerderechts bei einer Aufsichtsbehörde**;
- Information, **ob die Datenbereitstellung** der Daten gesetzlich oder vertraglich **vorgeschrieben bzw.** vertraglich **erforderlich ist** und ob eine Verpflichtung zur Bereitstellung besteht sowie Folgen der Nichtbereitstellung;
- Information zum Bestehen einer automatisierten Entscheidungsfindung / Profiling, dazu Entscheidungslogik, Tragweite und Auswirkung der Datenverarbeitung auf den Betroffenen.

Nach Art. 14 DS-GVO bestehen ähnliche Informationspflichten, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden.

- **Einstufung,** in welcher datenschutzrechtlichen **Rolle** erfolgt die Verarbeitung der Daten (Eigentümer, Verwalter, Vermittler)?
- Erfolgt die Verarbeitung ggf. als **Auftragsverarbeiter** nach Art 28 DS-GVO, handeln Vermittler und Eigentümer ggf. als **gemeinsam für die Verarbeitung Verantwortliche** nach Art. 26 DS-GVO oder sind Beide **jeweils Verantwortliche** der Datenverarbeitung?
- **Prüfung**, ob in etwaige **Übermittlungen** an den Eigentümer oder weiteren Dritten **eingewilligt wurde**?
- **Prüfung**, wer die **Bonitätsabfrage** zulässiger Weise einholen und nutzen darf? (Ich/Wir sind damit einverstanden, dass der Vermieter bei der SCHUFA Holding AG, Wiesbaden die Schufa- Verbraucherauskunft zum Zwecke der Vermietung einholt. Auf Wunsch kann auch eine SCHUFA Selbstauskunft vorgelegt werden.
- Ist eine **Personalausweiskopie** erforderlich, ist ein **digitale Weiterverarbeitung** und gar **Übermittlung** zulässig – oder reicht eine Identitätsfeststellung aus?

Sicherheit der Verarbeitung

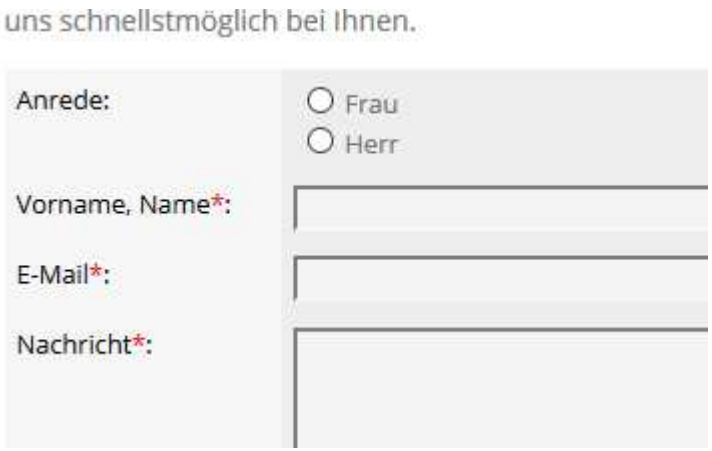
Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

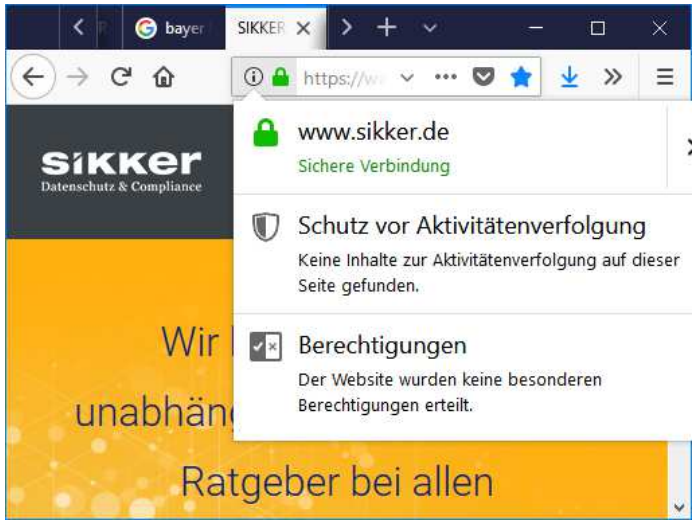
Die Maßnahmen sollen dazu führen, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden.

Transport- und Übertragungskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektroni-*schen 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.*

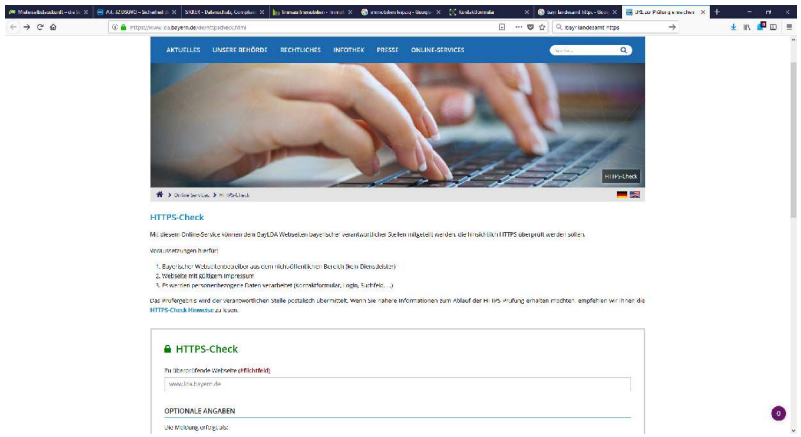
Auszug aus § 13 TMG „Eine Maßnahme nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens“.

Datenerhebung über Kontaktformular im Internet





sikker
Datenschutz & Compliance



Bayerisches Landesamt für Datenschutzaufsicht

Ablauf der Überprüfung der HTTPS-Verschlüsselung einer Webseite

1. **Objekt der Prüfung**
   Das BayLDA untersucht sowohl Webseiten, deren URLs eigenständig erhoben wurden, als auch die, die von den Webseitenbetreibern selbst oder von Dritten dem BayLDA mitgeteilt worden sind (z. B. per E-Mail oder über den neuen Online-Service „HTTPS-Check").

2. **Gegenstand der Prüfung**
   Geprüft wird, ob die Webseiten über eine ausreichende HTTPS-Verschlüsselung verfügen, um den Datentransfer zwischen dem Browser des Nutzers und dem Internet-Server des Anbieters abzusichern. Dies gilt besonders für Webseiten, bei denen Kontakt- und Zahlungsdaten eingegeben werden können (z. B. Online-Shops), sowie für Webseiten von Unternehmen, die ein Kontaktformular als mögliches Kommunikationsmedium anbieten. Darüber hinaus kann in Einzelfällen auch bei anderen Webseiten eine HTTPS-Verschlüsselung erforderlich sein, da weitere Nutzungsdaten verarbeitet werden.

4. Umgang mit dem Ergebnis der Prüfung

Alle Unternehmen, deren Webseiten von uns überprüft wurden, erhalten einen kurzen automatisch generierten Prüfbericht. Soweit die Webseiten über eine ausreichende Verschlüsselung verfügen, wird dies entsprechend schriftlich bestätigt. Sollten jedoch Mängel durch die Prüfung erkannt werden, so werden diese dem Betreiber mit der Aufforderung mitgeteilt, innerhalb einer Frist die erforderlichen Maßnahmen zur Verschlüsselung umzusetzen. Sofern Betreiber von Webseiten ohne ausreichende Begründung der Verpflichtung, eine angemessene Ver-schlüsselung vorzusehen, nicht nachkommen, wird das BayLDA durch eine entsprechende Anordnung die Betreiber verpflichten, die Verschlüsselung zu implementieren und, falls dieser Anordnung nicht nachgekommen wird, gege-benenfalls ergänzend einen Bußgeldbescheid gegen den Verantwortlichen erlassen.

Verschlüsselter Versand personenbezogener Daten per E-Mail

Frank Hillmer [sikker.de] Testnachricht für IVD Mitte-Ost

Sehr geehrte Damen und Herren.... Viele Grüße Frank Hillmer SIKKER Datenschutz & Compliance I 04107 Leipzig Tel.+49 341 308246781 Fax.+49 341 308246788

FRANK HILLMER SIKKER Testnachricht für IVD Mitte-Ost

Kritisch insbesondere ist Übersendung von Vermögens- bzw. Einkunftsnachweisen, Mieterauskünften und Personalausweiskopien per E-Mail, bspw. an Eigentümer.

Sehr geehrter Herr XXX,

Ihre E-Mail vom XX. März 2018 haben wir erhalten.

Um in der Sache für Sie tätig zu werden (und Ihnen gegebenenfalls anschließend das Ergebnis unserer Überprüfung mitteilen zu können), benötigen wir

vorzugsweise Ihre Postanschrift oder alternativ Ihren öffentlichen PGP- oder S/MIME-Schlüssel.

Dies hat folgenden Hintergrund:

Wir haben die Verantwortung, dass die Informationen, die wir Ihnen zukommen lassen, auch bei ihrer Übermittlung vertraulich bleiben. Das unverschlüsselte Übermitteln von personenbezogenen Informationen in einer E-Mail im Internet ist mit erheblichen Risiken verbunden. So ist es unbefugten Personen unter Umständen ohne großen Aufwand möglich, unbemerkt eine unverschlüsselte E-Mail zu lesen und inhaltlich nach Belieben abzuändern. Die unverschlüsselte E-Mail ist letztlich einer per Bleistift geschriebenen Postkarte vergleichbar.

Als Berliner Beauftragte für Datenschutz und Informationsfreiheit kontrollieren wir die Einhaltung der datenschutzrechtlichen Vorschriften im Land Berlin. Dementsprechend ist uns die datenschutzgerechte Bearbeitung von Eingaben ein besonders wichtiges Anliegen. Bitte haben Sie Verständnis für diese Vorgehensweise, die ausschließlich dem Schutz Ihrer personenbezogenen Daten dient.

Wenn Sie die elektronische Kommunikation trotz der mit ihr verbundenen Risiken bevorzugen, dann senden Sie uns bitte Ihre Eingabe erneut in einer elektronisch signierten Nachricht und legen Ihren öffentlichen PGP- oder S/MIME-Schlüssel bei. Welche Eigenschaften dieser Schlüssel haben muss, damit er sich für den Schutz der Nachrichten eignet, haben wir in dem beiliegenden Merkblatt dargelegt. Bitte haben Sie Verständnis dafür, dass wir Schlüssel, die den Anforderungen nicht genügen, zurückweisen müssen.

Sollten Sie Ihre E-Mail nicht als Sie persönlich betreffende Eingabe, sondern vielmehr als Hinweis auf einen bestimmten Sachverhalt verstanden wissen möchten, werden wir die von Ihnen geschilderte Angelegenheit gegebenenfalls im Rahmen unserer begrenzten Kapazitäten von Amts wegen überprüfen, allerdings keinen weiteren Schriftverkehr mit Ihnen führen. Wir bitten hierfür um Ihr Verständnis.

Mit freundlichen Grüßen

Ihre Servicestelle Bürgereingaben

Berliner Beauftragte für
Datenschutz und Informationsfreiheit
Bereich Recht II

Verzeichnis von Verarbeitungstätig-keiten

Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

- den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
- die Zwecke der Verarbeitung;
- eine 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…;
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation….
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

Sanktionen

Womit müssen Sie rechnen, wenn Sie das Datengeheimnis nicht wahren?

nach DS-GVO

bspw. Verstoß gegen Artikel 30 - Verzeichnis von **Verarbeitungstätigkeiten**

bis zu **10 Mio. EUR** oder **2%** des weltweiten Umsatzes

bspw. z.B. Verstoß gegen Artikel 7 - **Einwilligungserklärungen**

bis zu **20 Mio. EUR** oder **4%** des weltweiten Umsatzes

nach BDSG

Mit **Freiheitsstrafe bis zu drei Jahren** oder mit Geldstrafe wird bestraft, wer **wissentlich** nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,
1. einem Dritten übermittelt oder
2. auf andere Art und Weise zugänglich macht und hierbei gewerbsmäßig handelt.

Mit **Freiheitsstrafe bis zu zwei Jahren** oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,
1. ohne hierzu berechtigt zu sein, verarbeitet oder
2. durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

Vielen Dank für Ihre Aufmerksamkeit

SIKKER Datenschutz & Compliance
Frank Hillmer
Emilienstr. 15, 04107 Leipzig
Tel. 0341 308246780
info@sikker.de