DATENSCHUTZ-GRUNDVERORDNUNG

INHALTSVERZEICHNIS

AB 25. MAI GELTEN NEUE VORSCHRIFTEN BEIM DATENSCHUTZ: WAS SIE JETZT TUN MÜSSEN

1. ALLGEMEIN

Mit Stichtag 25. Mai 2018 gilt die neue Datenschutz-Grundverordnung der EU. Ihre inhaltlichen Anforderungen ähneln vielfach dem derzeit geltenden Recht. Gleichwohl bringt sie auch zusätzliche Pflichten mit sich. Zudem drohen bei Verstößen gegen die Vorgaben des Datenschutzes deutlich härtere Sanktionen.

1.1. DATENSCHUTZ WIRD NOCH WICHTIGER

Einhaltung des Datenschutzes muss nachgewiesen werden

Bereits jetzt muss der Datenschutz gewahrt werden: gesetzliche Grundlagen sind insbesondere das Bundesdatenschutzgesetz. Nach der Datenschutz-Grundverordnung (DSGVO) sind sie künftig auch verpflichtet nachzuweisen, dass sie die datenschutzrechtlichen Grundsätze einhalten, zum Beispiel gegenüber den Aufsichtsbehörden. Außerdem kommen neue Informationspflichten gegenüber den Betroffenen hinzu.

DSGVO gilt für alle!

Die DSGVO gilt für den gesamten öffentlichen Bereich, also für private Unternehmen, öffentliche Stellen, freiberuflich Tätige oder Vereine. Sie vereinheitlicht die Regeln zur Verarbeitung personenbezogener Daten.

1.2. UM DIESE DATEN UND IHREN SCHUTZ GEHT ES

Was die „Verarbeitung“ von Daten alles umfasst

Unter dem Begriff „Verarbeiten“ werden alle Tätigkeiten zusammengefasst wie Erheben und Abfragen, Ordnen, Speichern, Anpassen und Ändern, Auslesen und Weiterleiten, Löschen und Vernichten der Daten. Dieser Prozess beginnt meist bei der Anfrage.

Es geht um personenbezogene Daten

Gesetzlich definiert wird der Begriff “personenbezogene Daten” in Artikel 4 der DSGVO als “alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person […] beziehen”.

Grundsätzlich fallen alle Daten unter die personenbezogenen Daten, mit deren Hilfe ein Personenbezug hergestellt werden kann.

Klassisch gehören dazu also beispielsweise:

- Name
- Adresse
- Telefonnummer
- die Kreditkarten- oder Personalnummer
- Kontodaten
- Online-Daten wie IP-Adresse oder Standortdaten

Und auch physische Daten wie das Aussehen fallen unter die personenbezogenen Daten. Darüber hinaus sind es Sachverhalte wie die Staats- oder Religionszugehörigkeit oder eine Mitgliedschaft in einem Verein.

2. AUF EINEN BLICK: DAS IST IN PUNCTO DATENSCHUTZ JETZT ZU TUN

Die folgende Übersicht führt auf, was vorgehalten werden muss, um der Informations- und Nachweispflicht nach der DSGVO gerecht zu werden. Auf den nachfolgenden Seiten werden die Punkte näher erläutert.

2.1. WAS MAN AB 25. MAI BENÖTIGT

Übersicht

Alle:

- Verzeichnis von Verarbeitungstätigkeiten, die auf Verlangen der Aufsichtsbehörde vorgelegt werden muss
- Aufstellung der technischen und organisatorischen Maßnahmen, die zum Schutz von personenbezogenen Daten ergriffen werden
- Vereinbarung zur Auftragsverarbeitung mit Softwareanbietern und anderen Dienstleistern, wenn diese auf personenbezogene Daten z.B. Mitarbeiterdaten zugreifen können
- Einen internen oder externen Datenschutzbeauftragten, wenn mindestens zehn Personen regelmäßig personenbezogene Daten automatisiert verarbeiten, zum Beispiel am Empfang

Darüber hinaus kann dies erforderlich sein:

- In seltenen Fällen kann eine Datenschutz-Folgenabschätzung nötig sein, zum Beispiel wenn große Mengen an personenbezogenen Daten verarbeitet oder die Räume systematisch videoüberwacht werden.
- Einwilligungserklärungen, zum Beispiel für Weitergabe von Daten an eine privatärztliche Verrechnungsstelle, müssen um einen Hinweis auf Widerrufbarkeit ergänzt werden.
- Einrichtungen, die eine Internet- oder Facebook-Seite anbieten, sollten die Datenschutzerklärung prüfen und gegebenenfalls anpassen; dies gilt ebenso, wenn personenbezogene Daten zum Beispiel über Kontaktformulare oder für einen Newsletter erfasst und gespeichert werden.

3. HINWEISE UND EMPFEHLUNGEN ZUR UMSETZUNG

3.1. VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

Verzeichnis muss Aufsichtsbehörde auf Verlangen vorgelegt werden

In einem Verzeichnis von Verarbeitungstätigkeiten werden Tätigkeiten beziehungsweise Vorgänge erfasst, bei denen personenbezogene Daten verarbeitet werden. Die Aufstellung und Beschreibung der Tätigkeiten ist auf Verlangen der Aufsichtsbehörde bereitzustellen. Liegt kein Verzeichnis vor, drohen Geldstrafen.

3.1.1. DAS IST ZU TUN

So können Sie vorgehen:

- Schritt 1: Für das Erstellen des Verzeichnisses sollten Sie zunächst überlegen, wo überall personenbezogene Daten verarbeitet, also z.B. erhoben, gespeichert, bearbeitet oder weitergeleitet, werden. Dabei bietet es sich an, Tätigkeiten, die demselben Zweck dienen, zusammenzufassen.
  Eine Tätigkeit, die in vielen Unternehmen anfallen dürfte, ist das Führen von Personalakten, um Mitarbeiter beschäftigen zu können.

  Tätigkeiten, bei denen Daten verarbeitet werden, zusammenstellen

- Schritt 2: Im nächsten Schritt fügen Sie zu jeder Tätigkeit die in der DSGVO geforderten Angaben hinzu.
  Das sind:
  - Zweck der Verarbeitung (z.B. Gehaltsabrechnung)
  - betroffene Personengruppen (z.B. Beschäftigte)
  - Datenkategorien (z.B. Personaldaten)
  - Empfängergruppen, gegenüber denen die personenbezogenen Daten offengelegt werden (z.B. Krankenkassen)
  - Fristen für die Löschung (z.B. zehn Jahre)

  Datenübersicht – Wer macht was mit welchen Daten

  Angaben zu den Tätigkeiten

- Schritt 3: Geben Sie jetzt noch den Namen und die Kontaktdaten Ihres Unternehmens und gegebenenfalls des Datenschutzbeauftragten an.
  Prüfen Sie bei der Erstellung des Verzeichnisses auch, ob bestimmte Datenverarbeitungsvorgänge ein besonders hohes Risiko bergen. Dann könnte unter Umständen eine Datenschutz-Folgenabschätzung nötig sein

  Angaben zur Einrichtung

- Art. 5 Abs. 2 DSGVO schreibt vor, dass der für die Verarbeitung Verantwortliche nachweisen können muss, dass er die in Art. 5 Abs. 1 DSGVO geregelten Datenschutzgrundsätze einhält. Verstößt ein verantwortliches Unternehmen gegen diese Vorgabe, drohen **Bußgelder von bis zu 4 Prozent des Umsatzes.**

  Bußgeld: bis zu 4 Prozent des Umsatzes

3.2. AUFSTELLUNG DER MAßNAHMEN ZUM DATENSCHUTZ

Unternehmen sind für den Schutz personenbezogener Daten verantwortlich. Sie müssen dazu geeignete technische und organisatorische Maßnahmen ergreifen und diese dokumentieren. So kennen alle Mitarbeiter die Regeln, und bei externen Kontrollen oder Anfragen kann der interne Datenschutzplan vorgelegt werden.

Interne Regeln zum Umgang mit sensiblen Daten

3.2.1. DIESE MAßNAHMEN ZUM DATENSCHUTZ GEHÖREN DAZU

Die DSGVO macht keine konkreten Vorgaben, welche Maßnahme im Einzelnen dokumentiert werden soll. Doch letztlich geht es darum, zu erfassen, welche Vorkehrungen getroffen wurden, um einen Missbrauch von personenbezogenen Daten zu verhindern.

Maßnahmen zum Datenschutz

Auf diese Punkte kommt es insbesondere an:

- Pseudonymisierung und **Verschlüsselung** personenbezogener Daten. Emails mit personenbezogenen Daten NIE unverschlüsselt versenden
- **Zugriffsberechtigungen** vergeben; somit ist klar geregelt, wer auf Dateien und Ordner zugreifen kann.
- Personalakten **sicher** verwahren: PCs sind passwortgeschützt, die automatische Bildschirmsperre ist aktiviert. Wenn niemand im Raum ist, werden Personenakten generell unter Verschluss gehalten.
- Es ist festgelegt, was bei Datenpannen und Datenschutzverstößen zu tun ist und wer die Meldung übernimmt
  (innerhalb von 72 Stunden an die zuständige Aufsichtsbehörde).
- Die Mitarbeiter wurden über die Einhaltung von **Schweigepflicht** und Datenschutz informiert.
- Es dürfen nur die Daten gespeichert werden, die auch wirklich benötigt werden. (**Datenminimierung**)
- Zudem sollte grundsätzlich sichergestellt sein, dass Unbefugte keinen Zutritt erhalten. Auch zulässige Besucher sollten stets empfangen und registriert werden (**Zugangskontrolle**).
- Verstöße gegen das Gebot „**Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen zu gewährleisten“ und gegen die Datensicherheit**, können mit Bußgeldern von bis zu 2 Prozent des Umsatzes des Unternehmens geahndet werden.

Bußgeld: bis zu 2 Prozent des Umsatzes

- Es ist festzulegen, wann und durch wen personenbezogene Daten gelöscht bzw. vernichtet werden (**Löschfristen**).
  - Der Verantwortliche muss personenbezogene Daten ohne unangemessene Verzögerung löschen, sofern einer der in Art. 17 Abs. 1 DSGVO genannten Gründe zutrifft. Die wichtigsten Gründe sind:
    - Der Zweck für die Datenverarbeitung ist weggefallen
    - Der Betroffene hat seine Einwilligung
    - Die Datenverarbeitung war unrechtmäßig

Bußgeld: bis zu 4 Prozent des Umsatzes

3.3. AUFTRAGSVERARBEITUNG: ZUSAMMENARBEIT MIT DIENSTLEISTERN

Die EDV wird gewartet, Akten- und Datenträger müssen nach Ablauf der Aufbewahrungsfrist vernichtet werden. Immer dann, wenn ein externer Dienstleister auf Mitarbeiterdaten zugreifen kann, ist der Abschluss eines Vertrages zur Auftragsverarbeitung (als Anlage zum Hauptvertrag) erforderlich.

Die Auftraggeber müssen sich ferner davon überzeugen, dass der Dienstleister die Vorschriften des Datenschutzes einhält und entsprechende technische und organisatorische Maßnahmen durchführt. Die Firmen sollten dem Auftragsnehmer dazu ein Datenschutzsiegel oder eine Zertifizierung, zum Beispiel ISO/IEC 27001, vorlegen.

3.3.1. AUFTRAGSVERARBEITUNG: JA ODER NEIN?

Beispiel für Auftragsverarbeitung

Eine Auftragsverarbeitung liegt nicht nur bei der Wartung der EDV oder der Akten- und Datenträgervernichtung vor. Weitere Beispiele sind die Nutzung von Cloud-Systemen und die Terminvergabe durch Externe. Dagegen ist eine rein technische Wartung der IT-Infrastruktur durch einen Externen, z.B. Arbeiten an der Stromzufuhr, Kühlung oder Heizung, keine Auftragsverarbeitung. Dies gilt ebenso bei der Beauftragung von Steuerberatern, Rechtsanwälten, Wirtschaftsprüfern und Angehörigen anderer Berufe, die als „Geheimnisträger“ gelten. Auch hier liegt in der Regel keine Auftragsverarbeitung vor.

3.3.2. DAS IST ZU TUN

Vertrag zur Auftragsverarbeitung abschließen

Schritt 1: Schauen Sie zunächst, ob Sie für Ihre Dienstleistungsverträge (z.B. zur Wartung der EDV) jeweils einen Vertrag zur Auftragsverarbeitung haben, und passen Sie diesen in Abstimmung mit dem Auftragnehmer gegebenenfalls an.

Schritt 2: Ist das nicht der Fall, sprechen Sie Ihren Dienstleister an. Er benötigt einen Vertrag zur Auftragsverarbeitung und wird Ihnen in der Regel einen Entwurf zusenden.

3.3.2.1. FOLGENDE INHALTE SOLLTE DER VERTRAG ENTHALTEN:

Das sollte der Vertrag enthalten

- Gegenstand und Dauer der Verarbeitung (um welche Leistung handelt es sich, wie lange wird diese beauftragt)
- Art und Zweck der Verarbeitung (wozu dient sie, welches Ziel soll erreicht werden)
- Art der personenbezogenen Daten und Kategorien betroffener Personen (z.B. Zugriff auf Gesundheitsdaten)
- Rechte und Pflichten des Auftraggebers sowie dessen Weisungsbefugnisse
- Verpflichtung der zur Verarbeitung berechtigten Personen zur Vertraulichkeit
- Benennung der technischen und organisatorischen Maßnahmen, die das Unternehmen zum Schutz personenbezogener Daten durchführt (z.B. Einhaltung von Vorgaben der ISO/IEC 27001)
- Verpflichtung des Auftragnehmers zur Unterstützung des Auftraggebers bei:
    - Anfragen und Ansprüchen Betroffener im Zusammenhang mit der Auftragsverarbeitung
    - der Meldepflicht bei Datenschutzverletzungen und der Datenschutz-Folgenabschätzung

- Rückgabe oder Löschung personenbezogener Daten nach Abschluss der Auftragsverarbeitung
- Verpflichtung des Auftragnehmers, dem Auftraggeber alle Informationen zum Nachweis der Einhaltung der datenschutzrechtlichen Pflichten bereitzustellen.

Schritt 3: Lassen Sie sich vom Dienstleister ein geeignetes Zertifikat, zum Beispiel ISO/IEC 27001, vorlegen. Das Zertifikat dient dem Nachweis der eingesetzten technischen und organisatorischen Maßnahmen zum Schutz der Daten beim Auftragnehmer. Eine weitergehende Pflicht zur Kontrolle durch Sie besteht nicht.

Nachweis des Auftragnehmers zur Einhaltung des Datenschutzes

3.4. DATENSCHUTZBEAUFTRAGTEN BENENNEN – AB 10 PERSONEN

Größere Einrichtungen benötigen einen Datenschutzbeauftragten. Wie bisher ist dies Pflicht, wenn mind. 10 Personen regelmäßig Daten automatisiert – z.B. am PC – verarbeiten.

Die Aufgabe des Datenschutzbeauftragten kann ein fachlich qualifizierter Mitarbeiter (nicht der Inhaber) oder ein externer Datenschützer übernehmen. Name und Kontaktdaten des Datenschutzbeauftragten müssen dem Landesdatenschutzbeauftragten mitgeteilt werden.

Mitteilung an Landesdatenschutzbeauftragten

Aufgabe des Datenschutzbeauftragten ist es, die Einhaltung des Datenschutzes und der Datensicherheit zu kontrollieren und geeignete Maßnahmen festzulegen. Er informiert und berät über ihre Pflichten nach dem Datenschutzrecht. Darüber hinaus ist er Ansprechpartner für die Aufsichtsbehörde.

Aufgaben des Datenschutzbeauftragten

3.5. DATENSCHUTZ-FOLGENABSCHÄTZUNG

Nur selten erforderlich

In seltenen Fällen kann eine Datenschutz-Folgenabschätzung erforderlich sein, zum Beispiel wenn aufgrund des Umfangs und des Zwecks der Datenverarbeitung ein hohes Datenschutzrisiko besteht. Auch eine systematische Videoüberwachung kann ein Grund sein.

Bestehen möglicherweise hohe Risiken bei der Datenverarbeitung, ist eine externe Datenschutzprüfung zu empfehlen. Sollten Sie Zweifel haben, ob dies im Einzelfall nötig ist, empfiehlt es sich, dies beim Landesdatenschutzbeauftragten zu erfragen.

3.6. EINWILLIGUNGSERKLÄRUNGEN ANPASSEN

Sind Speicherung, Nutzung und Verarbeitung personenbezogener Daten nicht aufgrund einer gesetzlichen Grundlage gestattet oder geboten, ist dies nur mit der Einwilligung des Betroffenen zulässig.

Die Einwilligungserklärung muss dabei grundsätzlich eindeutig als solche erkennbar sein und muss neben dem Hinweis auf den jeweiligen Verwendungszweck auch die Rechte des Betroffenen auf Löschung, Auskunft und Widerspruch aufführen.

Fehlt die Einwilligung des Betroffenen in einem solchen Falle und die Daten werden dennoch unzulässigerweise erhoben, so handelt es sich um einen Datenschutzverstoß.

3.6.1. DAS IST ZU TUN

Gemäß Datenschutz muss die Einwilligungserklärung für den Betroffenen eindeutig als solche identifiziert werden können.

Dem Betroffenen muss eindeutig dargelegt werden, zu welchem Zweck die jeweilige öffentliche oder nicht öffentliche Stelle die einzelnen Daten abfragt und nutzen möchte.

Ab 25. Mai müssen Einwilligungserklärungen einen Hinweis darauf enthalten, dass

- Betroffene ihr Einverständnis jederzeit widerrufen können
- die Abgabe der Einwilligungserklärung in jedem Fall freiwillig erfolgt
- Recht auf Löschung, Sperrung und Berichtigung

Ergänzen Sie gegebenenfalls Ihre Vorlagen.

3.7. DATENSCHUTZERKLÄRUNG AUF DER INTERNETSEITE

Zahlreiche Einrichtungen haben eine Internet- oder Facebook-Seite. Terminerinnerungen per SMS oder Newsletter gehören zunehmend zum Service. Auch dabei werden personenbezogene Daten verarbeitet, die geschützt werden müssen.

3.7.1. DAS IST ZU TUN

Hinweise zum Datenschutz auf der Webseite

Prüfen Sie, ob auf Ihrer Internet- oder Facebook-Seite eine Datenschutzerklärung eingestellt ist und diese alle nötigen Angaben beinhaltet. Außerdem können Sie die Informationen zum Datenschutz auf Ihre Internetseite stellen.

Weisen Sie in der Datenschutzerklärung unter anderem darauf hin, dass

- personenbezogene Daten wie Name, Postanschrift, E-Mail-Adresse, Telefonnummer oder das Geburtsdatum ausschließlich in Übereinstimmung mit dem jeweils geltenden Datenschutzrecht erhoben und genutzt werden
- die Daten nur gespeichert werden, wenn sie aktiv übermittelt werden
- die Daten zum Beispiel nur zur Beantwortung von Anfragen oder zur Zusendung von Informationsmaterial verwendet werden
- Kontaktdaten, die im Rahmen von Anfragen angegeben werden, ausschließlich für die Korrespondenz verwendet werden
- E-Mail-Adressen, die Nutzer für den Bezug eines Newsletters angegeben haben, nur dafür genutzt werden

3.8. DATENPORTABILITÄT

Die EU-DSGVO bringt in Art. 20 (Datenportabilität) für die Betroffenen ein „Recht auf Herausgabe und Übertragung ihrer personenbezogenen Daten“. Betroffene können nunmehr verlangen, dass ihre Daten an eine neue Bank, einen Arbeitgeber, Arzt oder Pflegedienst übertragen werden. Die Übertragung muss dabei ohne Behinderung erfolgen, das heißt, die Datenübertragung ist nicht an Bedingungen zu knüpfen; insbesondere hat die Übermittlung der Daten entsprechen Art. 12 Abs. 5 EU-DSGVO in der Regel unentgeltlich zu erfolgen hat. Dabei soll die technische Datenübertragung der personenbezogenen Daten durch ein „strukturiertes, gängiges, maschinenlesbares und interoperables Format“ erfolgen.

Recht auf Herausgabe und Übertragung der Daten

Die Ablehnung der Datenübertragung fällt unter den Tatbestand des Art. 83 Abs. 5 EU-DSGVO. Dieser sieht als Sanktionsmöglichkeit ein Bußgeld in Höhe von 20 Millionen Euro bzw. bis zu 4% des weltweit erzielten Jahresumsatzes des vergangenen Geschäftsjahres vor.

Bußgeld: bis zu 4 Prozent des Umsatzes

3.9. BEI VERSTÖßEN DROHEN HOHE GELDSTRAFEN

Das Ausmaß der Sanktionen richtet sich vor allem nach der Schwere und der Dauer des Vorfalls sowie nach dessen Auswirkungen auf die Betroffenen. Leichte Verstöße werden zunächst zu einer Beratung führen.

Dennoch sollten alle nötigen Vorkehrungen getroffen werden. Denn die DSGVO sieht bei Verstößen generell deutlich härtere Sanktionen vor als sie bisher üblich sind. Die Aufsichtsbehörden – in der Regel die Landesdatenschutzbeauftragten – können im Einzelfall Geldbußen von bis zu 20 Millionen Euro verhängen. Möglich sind zudem Schadensersatzforderungen von Betroffenen inklusive Schmerzensgeld, zum Beispiel wegen Rufverletzung.

3.10. WIE KOMMT EIN AHNDUNGSWÜRDIGER SACHVERHALT ANS LICHT?

- durch proaktive Überprüfungstätigkeit der Aufsichtsbehörden
- durch einen unzufriedenen Mitarbeiter, der sich bei der Aufsichtsbehörde beschwert
- durch Kunden oder potentielle Kunden, die eine Meldung bei der Aufsichtsbehörde machen
- durch Selbstanzeige des Unternehmens
- durch die Presse im Allgemeinen, insbesondere auch Investigativjournalismus