

Neues Datenschutzrecht umsetzen

Stichtag 25.05.2018

Rechtsanwalt Arnt Kotulla

Vortrag am 22.03.2018

IHK für das östliche Mecklenburg-Vorpommern Neubrandenburg

Was ist Datenschutz?

- Schutz den Menschen
 - Meinungsfreiheit
 - Informationsfreiheit
 - Entscheidungsfreiheit
-
- Recht aus Informationelle Selbstbestimmung
 - Art. 2 Abs. 1, Art. 1 Abs. 1 GG, Art. 8 EMRK, Art. 8 EU Grundrecht-Charta

Notwendige Schritte bis 25.05.2018

- Einhaltung neuer Datenschutzgrundsätze und deren Dokumentation
- Verwendung neuer Auftragsdatenverarbeitungsverträge
- Verwendung neuer Datenschutzinformationen online
- Datensicherheit auf Risikobasis umstellen TOM's
- Umstellung auf interne pseudonymisierte Verarbeitung
- Maßnahmen für neue Rechte
- Verfahrensverzeichnisse
- Schwellwertanalyse
- Musterauskunft

Neue abschreckende Geldbußen

- bis 20 Mio € / 4% Jahresumsatz
- bis 10 Mio € / 2% Jahresumsatz

Verstöße gegen

- Grundsätze der Verarbeitung
- Einwilligung
- Betroffenenrechte
- Übermittlung in Drittland
- Missachtung der Aufsicht

Verstöße gegen

- Auftragsdatenverarbeitung
- Verarbeitungsverzeichnisse
- Datensicherheit
- Privacy by Design
- Privacy by Default
- Meldepflichten
- Datenschutzbeauftragter

Grundsätze der Verarbeitung

Grundsätze der Verarbeitung von Personenbezogenen Daten nach Art. 5 DSGVO

Grundsatz	Bedeutung
1 Rechtmäßigkeit	auf rechtmäßige Weise, ohne Gesetzesverstoß
2 Treu und Glauben	Verarbeitung der personenbezogenen Daten nach Treu und Glauben ohne Täuschung des Betroffenen
3 Transparenz	in einer für die betroffene Person nachvollziehbaren Weise, durch Informationen über die Verarbeitung
4 Zweckbindung	festgelegte, eindeutige und legitime Zwecke und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeiten
5 Datenminimierung	dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt
6 Richtigkeit	sachlich richtig
7 Speicherbegrenzung	nur so lange wie erforderlich
8 Integrität und Vertraulichkeit	Technisch Organisatorische Maßnahmen
9 Rechenschaftspflicht	Einhaltung nachweisen

Bußgelder bis 4%
Jahresumsatz oder
20 Mio € bei Verstoß

Betroffenenrechte

- Recht auf Auskunft und Kopie der personenbezogenen Daten
 - Recht auf Berichtigung
 - Recht auf Löschung
 - Recht auf Einschränkung der Verarbeitung
 - Recht auf Datenportabilität
-
- gegen Verantwortlichen und Verarbeiter
-
- Bei Verstößen bis 4% Jahresumsatz bzw. 20 Mio €

Einwilligung in die Verarbeitung

- informierte Einwilligung mit konkreter Beschreibung der Verarbeitung und des Zweckes
- freiwillige Einwilligung, der Betroffene darf nicht einem Zwang unterliegen, etwa durch die Koppelung an Gegenleistung
- Schufa Hinweis statt bisher Schufa Klausel
- werbefinanzierter FreeMailer mit Hauptleistungspflicht Datennutzung ...
Kunde zahlt mit seinen Personenbezogenen Daten

Datenübermittlung in Drittländer

- Sanktionen Geldbuße bis 20 Mio oder 4% Jahresumsatz
- Datenübermittlung zulässig ohne besondere Genehmigung der Aufsichtsbehörde, wenn
- Beschluss EU Kommission über angemessenes Schutzniveau vorliegt oder bestimmte geeignete Garantien

- Betroffen: Cloud , Newsletter, CRM, Kundenservice Chat
- USA, China, Russland,

Verzeichnis der Verarbeitungen

- Namen und die Kontaktdaten des Verantwortlichen sowie des DSB;
- Zwecke der Verarbeitung;
- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt einschließlich Empfänger in Drittländern oder internationalen Organisationen;
- Übermittlungen von Daten an ein Drittland sowie die Dokumentierung geeigneter Garantien;
- die vorgesehenen Fristen für die Löschung der Datenkategorien;
- allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Auftragsdatenverarbeitung

- Gegenstand und Dauer der Verarbeitung
- Art und Zweck der Verarbeitung
- Art der personenbezogenen Daten & Kategorien von betroffenen Personen
- Umfang der Weisungsbefugnisse
- Verpflichtung der zur Verarbeitung befugten Personen zur Vertraulichkeit
- Sicherstellung von technischen & organisatorischen Maßnahmen
- Hinzuziehung von Subunternehmern
- Unterstützung des Verantwortlichen bei Anfragen und Ansprüchen Betroffener
- Unterstützung des Verantwortlichen bei der Meldepflicht bei Datenschutzverletzungen
- Rückgabe oder Löschung der Daten nach Abschluss der Auftragsdatenverarbeitung
- Kontrollrechte des Verantwortlichen und Duldungspflichten des Auftragsverarbeiters
- Pflicht des Auftragsverarbeiters, den Verantwortlichen zu informieren, falls eine Weisung gegen Datenschutzrecht verstößt

Technisch-organisatorische Maßnahmen

1. Vertraulichkeit

>> Zutrittskontrolle >> Zugangskontrolle >> Zugriffskontrolle >> Trennungskontrolle
>> Pseudonymisierung

2. Integrität

>> Weitergabekontrolle >> Eingabekontrolle

3. Verfügbarkeit und Belastbarkeit

>> Verfügbarkeitskontrolle

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

>> Datenschutz-Management; >> Incident-Response-Management; >> Datenschutzfreundliche Voreinstellungen >> Auftragskontrolle

Schwellwertanalyse und Datenschutzfolgeabschätzung

- Sanktionen Geldbuße bis 10 Mio bzw. 2 % Jahresumsatz

Die Schwellwert-Analyse dient dem Verantwortlichen als Entscheidungsgrundlage, ob eine Datenschutzfolgenabschätzung (DSFA) notwendig ist.

Eine DSFA ist notwendig bei einem hohem Risiko für die Rechte und Freiheiten von Betroffenen. Dies ist gegeben, wenn eine hohe Eingriffsintensität durch eine Form der Verfahrenstätigkeit vorliegt.

Soweit die DSFA nicht grundsätzlich durchzuführen ist, hilft die Schwellwert-Analyse bei der Entscheidung. Dazu werden die Risiken die sich aus einer einzelnen Verfahrenstätigkeit ergeben bewertet. Liegt ein hohes Risiko vor, ist die DSFA notwendig.

Notwendige Schritte bis 25.05.2018

- Einhaltung neuer Datenschutzgrundsätze und deren Dokumentation
- Verwendung neuer Auftragsdatenverarbeitungsverträge
- Verwendung neuer Datenschutzinformationen online
- Datensicherheit auf Risikobasis umstellen TOM's
- Umstellung auf interne pseudonymisierte Verarbeitung
- Maßnahmen für neue Rechte
- Verfahrensverzeichnisse
- Schwellwertanalyse
- Musterauskunft

Wie die Datenschutzkanzlei hilft

- Beratung und Schulung
- Stellung Datenschutzbeauftragter
- Implementierung Datenschutzmanagementsystem
- Umsetzung Standarddatenschutzmodell
- Datenschutzfolgeabschätzung
- Mitarbeiterdatenschutz
- Fachtexte prüfen und erstellen (ADV, Datenschutzerklärung, online, Muster Auskunft)
- Penetrationstest
- Online Schulungsportal

W

Vielen Dank für Ihre Aufmerksamkeit

