EUDSGVO

Natalie Wall
Fachanwältin für IT-Recht

www.unternehmen-und-datenschutz.de

NEUES EU-DATENSCHUTZRECHT

Ab 25. Mai 2018 gilt das neue europäische Datenschutzrecht für alle Mitgliedstaaten

Die Bundesregierung hat nach 40 Jahren am 27.4.2017 das neue Bundesdatenschutzgesetz verabschiedet

Bei Verstößen gegen das neue Datenschutzecht drohen Bußgelder

Bußgelder bis zu 20 Mio. € oder 4% des Konzernjahresumsatzes

Auch Auftragsdatenverarbeiter/Subunternehmer sind betroffen, für sie gelten ebenfalls weitreichende Neuerungen

EUDSGVO - NEUES EU-DATENSCHUTZRECHT

Was ist NEU ?

NEU Kategorisierung Datenschutzrelevanter Prozesse und Dokumentation durch das Unternehmen selbst

=> Führen eines Verfahrensregisters - alle datenschutzrelevanten Vorgänge müssen registriert werden

NEU Datenschutzfolgenabschätzung (DSFA)

=> Das Unternehmen muss selbst eine **Risikobewertung** vornehmen, wieweit Prozesse oder Projekte Auswirkungen auf den Datenschutz im Unternehmen haben; insbesondere bei Verwendung neuer Technologien. Unternehmen hat neuerdings eine Meldepflicht ggü der DS-Behörde.

Kriterien für eine Datenschutz-Folgenabschätzung (DSFA)

Insbesondere bei folgenden Datenverarbeitungsvorgänge (es müssen idR zwei Kriterien erfüllt sein):

- Daten zur Bewertung, zum Scoring oder zum Profiling, insbesondere in den Bereichen Arbeit, wirtschaftliche Situation, Gesundheit, persönliche Vorlieben und Interessen, Bonität, Verhaltensweisen, Aufenthaltsort;
- Formen automatisierter Entscheidungsfindung mit rechtlichen Folgen;
- Verarbeitung sensibler Daten wie beispielsweise Gesundheitsdaten;
- umfangreiche Verarbeitungsvorgänge;
- zusammengeführte oder kombinierte Datensätze;
- Daten schutzbedürftiger Personen wie Kindern, älteren Menschen, Patienten oder Mitarbeitern;

Kriterien für eine Datenschutz-Folgenabschätzung (DSFA)

Fortsetzung:

- Nutzung neuer Technologien wie IoT-Entwicklungen *(Internet of Things-Anschluss v. Anlagen ans Internet, M2M Kommunikation)*;
- Datentransfers außerhalb der EU;
- Datenverarbeitung kann dazu führen, dass ein Betroffener ein Recht nicht ausüben oder einen Vertrag nicht schließen kann (zB Prüfung auf Kreditwürdigkeit);

Rechtsfolge:

Wer eine DSFA nicht durchführt, obwohl er dazu verpflichtet war, riskiert Geldbußen von bis zu 10 Mio. € Euro oder bis zu 2% des gesamten weltweit erzielten Vorjahresumsatzes. Im Zweifel sollte deshalb eine Datenschutz-Folgenabschätzung durchgeführt und entsprechend dokumentiert werden

EUDSGVO - NEUES EU-DATENSCHUTZRECHT

Was ist NEU ?

NEU weite Informations-/Rechenschafts-/Meldepflichten der Unternehmen

- zB kurze Meldepflicht bei DS-Verletzungen: idR nur 72 Stunden Zeit, sonst Bußgeld; DSFA
- Stärkere Informationspflicht über den Umfang der Datenverarbeitung für Betroffene und neue Informationspflichten, zB zur Rechtsgrundlage der Datenverarbeitung oder der Speicherdauer.
- Dies hat Auswirkungen auf Einwilligungstexte, AGB und Datenschutzerklärungen müssen angepasst werden.

NEU Beweislastumkehr für Arbeitgeber

Der Arbeitgeber muss Einhaltung der datenschutzrechtlichen Vorgaben beweisen.

EUDSGVO - NEUES EU-DATENSCHUTZRECHT

Was ist NEU ?

NEU Sonderregelungen

– Sonderregelungen , zB Datenschutz am Arbeitsplatz, Videoüberwachung oder Profiling

NEU weitere Einbindung des Datenschutzbeauftragten

insbesondere bei:

– Beschwerden von Betroffenen (Mitarbeitern, Kunden)
– Einführung eines neuen Systems/Tools
– Einsatz eines neuen Dienstleisters
– Werbemaßnahmen (z.B. Versand von Newsletter)
– Onlinemarketing-Maßnahmen (Google AdWords, Conversion Tracking, etc.)
– Verkauf von Teilen des Unternehmens

EUDSGVO - NEUES EU-DATENSCHUTZRECHT

Was ist NEU ?

NEU Änderungen in der Auftrags(daten)verarbeitung

- => Geeignetheit: Auftragsverarbeiter muss hinreichend Garantien für geeignete technische und organisatorische Maßnahmen bieten, zB genehmigte Verhaltensregeln des Auftragsverarbeiters nach Art. 40 DS-GVO oder Zertifizierungen nach Art. 42 DS-GVO. Dann auch außerhalb EU-/*EWR*-Raum zulässig!
- **‚joint control'** Auftragsverarbeitungs-Auftraggeber und Auftragsverarbeiter haften gemeinsam; weitreichende gegenseitige Pflichten
- Schadensersatzansprüche (Schmerzensgeld) auch wegen Nichtvermögensschäden – Klagerecht Verbraucher und Verbände
- Neuerdings ist auch die Funktionsübertragung im Konzern als Auftragsverarbeitung erfasst!
- **Geldbußen bis zu 10 Mio.€ oder 2%** des Konzernjahresumsatzes

EUDSGVO - NEUES EU-DATENSCHUTZRECHT

Was ist NEU ?

NEU: kleines Konzernprivileg

=> Datenübermittlung im Konzernverbund: jede Konzerngesellschaft wird als externe Stelle betrachtet, doch bei berechtigtem Interesse ist die Datenübermittlung zulässig (kleines Konzernprivileg)

NEU: neue Anforderungen an die Datenübermittlung an Drittstaaten

Drittland muss ein angemessenes Datenschutzniveau haben:

- Beschluss der Europäischen Kommission
- Genehmigung von der zuständigen Aufsichtsbehörde
- Unterwerfung unter europäische Verhaltensregelungen

EUDSGVO - NEUES EU-DATENSCHUTZRECHT

Was ist NEU ?

NEU: neue Anforderungen an die Datenübermittlung an Drittstaaten

Fortsetzung:

Informationspflichten des Unternehmens, dass es die Daten an ein Drittland senden wird und auf welche Rechtsgrundlage es sich bei diesem Datentransfer beruft !

Auch Unternehmen, die ihren Sitz außerhalb haben, aber mit Daten von Unionsbürgern arbeiten, fallen unter den Schutz der DSGVO (Facebook, Google).

EUDSGVO - NEUES EU-DATENSCHUTZRECHT

Was ist NEU ?

NEU: EINWILLIGUNGSERKLÄRUNGEN

Bei Einwilligungserklärungen wird die Verarbeitung aufgrund überwiegender Interessen weniger möglich sein. Dies hat zur Folge, dass bestehende Verarbeitungsgrundlagen und geprüft und die Einwilligungserklärungen ggf. erneuert werden müssen.

NEU Technische Sicherheit - Bußgelder

Unternehmen müssen technische Sicherheitsvorkehrungen nachweisen können. Hierbei neue Anforderungen und Begrifflichkeiten zu beachten. Die konkreten Maßnahmen der Datensicherheit müssen außerdem dokumentiert werden. Fehlende oder unvollständige TOM´s (=technische und organisatorische Maßnahmen) können mit einem Bußgeld geahndet werden!

NEUE Anforderungen an die Unternehmen

DSGVO Compliance - was müssen Unternehmen tun ?

Datenschutzmanagementsystem

Die Unternehmen müssen einen Datenschutz-Management-Prozess implementieren.

Ein Datenschutzmanagementsystem wirkt bei versehentlichen Datenschutzverstößen bußgeldmindernd. Zudem ermöglicht ein effizientes System eine schnelle Reaktion bei einem Datenschutzverstoß.

Datenschutzmanagementsystem

Ein Datenschutzmanagementsystem muss die folgenden Anforderungen erfüllen:

- Verzeichnis von Verarbeitungstätigkeiten
- Datenschutzorganisation und Verantwortlichkeiten
- Datenschutz-Folgenabschätzung
- Vertragsmanagement
- Prozess für die Wahrnehmung von Betroffenenrechten
- Prozess für die Meldung von Datenschutzverstößen
- Nachweis der Datensicherheit

EUDSGVO - NEUES EU-DATENSCHUTZRECHT

Datenschutzmanagementsystem

Umsetzung

1. Prozesse und Tools für Datenschutzfolgenabschätzung (DSFA) implementieren, dh Instrumente, um die Risiken für den Datenschutz abzuschätzen und Abhilfemaßnahmen zur Bewältigung der Risiken (zB Anonymisieren, Datenmining, Datensparsamkeit)

2. Verfahrensregister führen: Hilfe zur Erfüllung der Rechenschaftspflicht

Risikobewertung (DSFA)

3. Auftragsdatenverarbeitung: Verträge und Strukturen zur

Auftragsdatenverarbeitung überarbeiten; sind bloße Funktionsübertragungen

eine verdeckte ADV? Kein Haftungsprivileg des Auftragsverarbeiters mehr - auch

der Auftragsdatenverarbeitung muss ein Verfahrensregister führen

Datenschutzmanagementsystem

Umsetzung

Fortsetzung

4. Kleines Konzernprivileg richtig ausgeübt (berechtigtes Interesse?)

5. Datenübermittlung an Drittstaaten (Schutzniveau eingehalten?)

6. Datensicherheit (technische und organisatorische Maßnahmen prüfen)

7. Bestehende Einwilligungen zur DV müssen überprüft werden

8. Einwilligungstexte, AGB und Datenschutzerklärungen müssen an erweiterte Informationspflichten angepasst werden.

Umsetzungsprozess

1. Internes Audit (Vergleich ist Zustand mit Sollzustand vor Ort im Unternehmen)

2. Prüfung, ob bisherige und fortgeltende Datenschutzgrundsätze richtig implementiert sind:

- Zweckbindung der DV („Zweckerweiterung“ nach Interessenabwägung)
- Datensparsamkeit (wenig, möglichst Pseudonymisierung und Anonymisierung bei DV)
- Datenrichtigkeit (falsche Daten sind unverzüglich zu löschen)
- Speicherungsfristen=> Löschkonzept

Umsetzungsprozess

Fortsetzung

3. Anpassung an die neuen Anforderungen

- Bestimmung Verantwortlichkeiten
- Bestimmung/Einbindung Datenschutzbeauftragten
- Erstellen Verfahrensregister
- Prozess/Tools zur Datenschutz-Folgenabschätzung
- Vertragsmanagement (externe Dienstleister, Datenübermittlung im Konzern)
- Mitarbeiterrichtlinien

Umsetzungsprozess

Fortsetzung

3. Anpassung an die neuen Anforderungen

- Datenschutz-Schulung für Mitarbeiter
- Prozess für die Wahrnehmung von Betroffenenrechten (Informationsrecht, Auskunfts- und Widerspruchsrecht, Recht auf Berichtigung, Löschung und Einschränkung, Recht auf Datenübertragbarkeit)
- internationaler Datentransfer
- Prozess für die Meldung von Datenschutzverstößen
- Nachweis der Datensicherheit

4. Schulung Mitarbeiter Datenschutz und IT-Sicherheit
(insb. Datenschutzfolgenabschätzung)

Risikoanalyse - Gefährdungsübersicht

Organisation

Personal

Infrastruktur

Technik

Risikoanalyse - Gefährdungsbewertung

Ausreichender Schutz durch Standardsicherheitsmaßnahmen?

- **Vollständigkeit** (Schutz gegen alle Gefährdungen?)

- **Mechanismenstärke** (ausreichender Schutz)

- **Zuverlässigkeit** (zB Umgehung des Schutzes?)

Risikomanagement - Erstellung Sicherheitskonzept

Eignung der Sicherheitsmaßnahmen

Zusammenwirken der Sicherheitsmaßnahmen

Benutzerfreundlichkeit der Sicherheitsmaßnahmen

Angemessenheit der Sicherheitsmaßnahmen

Managementsysteme - Komponenten

Sicherheitsprozesse

Mitarbeiter

Ressourcen

Managementprinzipien

Managementsysteme - Lebenszyklus

- Planung und Konzeption
- Beschaffung (falls erforderlich)
- Umsetzung
- Betrieb (Maßnahmen zur Aufrechterhaltung wie Überwachung und Erfolgskontrolle)
- Aussonderung (falls erforderlich)
- Notfallvorsorge

Managementsysteme - Phasen

- Planung
- Umsetzung der Planung bzw. Durchführung des Vorhabens
- Erfolgskontrolle bzw. Überwachung der Zielerreichung
- Beseitigung von erkannten Mängeln und Schwächen bzw. Optimierung sowie Verbesserung

Managementsysteme - Sicherheitskonzept

Erstellung s.o.:

- Gefährdungsanalyse

-Gefährdungsbewertung

Managementsysteme - Sicherheitskonzept

Umsetzung s.o.:

Sicherheitsprozesse

Mitarbeiter

Ressourcen

Managementprinzipien

Managementsysteme - Sicherheitskonzept

Erfolgskontrolle und Verbesserung des Sicherheitskonzepts

Reaktion auf Änderungen im laufenden Betrieb

Detektion von Sicherheitsvorfällen im laufenden Betrieb [DOK]

Überprüfung der Eignung und Wirksamkeit von Sicherheitsmaßnahmen [DOK]

Managementbewertungen

EUDSGVO - NEUES EU-DATENSCHUTZRECHT

Natalie Wall

Fachanwältin für IT-Recht

www.unternehmen-und-datenschutz.de

Wall&Kollegen

Karlsplatz 7
80335 München

FON 089 30 90 589-0
FAX 089 30 90 589-11
info@dsc.de
info@uud.de