



Bayerische
Forschungsallianz

Datenschutz im daily business

Thomas Eigner

(Datenschutzbeauftragter der BayFOR GmbH)





EU DS-GVO

Europäische Datenschutzgrundverordnung



Quelle: pixabay.com/de/photos/datenschutz



EU GDPR

European General Data Protection Regulation



Quelle: pixabay.com/de/photos/datenschutz



Das Wichtigste zur EU-Datenschutzgrundverordnung in Kürze

- Die neue europäische Datenschutzgrundverordnung trat bereits am 24. Mai 2016 in Kraft. Ab dem **25. Mai 2018** sind die hierin enthaltenen Maßgaben zum Datenschutz **verbindlich** in den jeweiligen Mitgliedstaaten anzuwenden – auch ohne die separate Übertragung in nationales Recht.
- Gestärkt werden sollen durch die europäische Datenschutzverordnung vor allem die **Verbraucherrechte**. Datenverarbeitende Stellen müssen mit strengeren Regulierungen rechnen.
- Ein **Verstoß gegen die EU-Datenschutzgrundverordnung** kann das betreffende Unternehmen bis zu **20 Millionen Euro Geldbuße** kosten – oder bis zu 4 % dessen weltweiter Umsätze (je nachdem, welcher Wert am Ende höher ausfällt).



Vergleich von Datenschutzrichtlinie und EU-Grundverordnung zum Datenschutz

- Am **24. Mai 2016** trat die neue EU-Datenschutzverordnung in Kraft. Seit dem **25. Mai 2018** EU DS-GVO in der gesamten EU und im EWR verbindlich anzuwenden. Das bedeutet für die Mitgliedstaaten der Europäischen Union: Sie müssen derzeit geltende nationale Gesetzesgrundlagen zum Datenschutz an die neue EU-Datenschutzgrundverordnung (DSGVO) sowie die **Strukturen in Behörden und Unternehmen** anpassen.
- Aber inwieweit **unterscheiden** sich in der EU-DSGVO getroffenen Regelungen zum Datenschutz von den derzeit noch gültigen Maßgaben der Richtlinie 95/46/EG? Was blieb gleich, was kam hinzu?



Vergleich von Datenschutzrichtlinie und EU-Grundverordnung zum Datenschutz

Im Folgenden finden Sie **elementare Bestandteile**, die grundlegend gleich geblieben sind sowie die wichtigsten Neuerungen:

Das ist geblieben

- Das maßgebliche Ziel der in der zum Datenschutz errichteten Grundverordnung der EU bleibt: Es sollen **die Grundrechte und Grundfreiheiten jeder natürlichen Person geschützt** werden – allen voran das Recht auf informationelle Selbstbestimmung.
- Als Grundsatz bleibt zudem bestehen, dass **personenbezogene Daten in aller Regel nicht erhoben oder verarbeitet werden dürfen**, sofern keine andere Rechtsvorschrift Abweichendes bestimmt. Ausnahmen müssen streng reguliert sein.
- Die Verarbeitung **besonders sensibler personenbezogene Daten** unterliegt auch nach der EU-Datenschutzgrundverordnung weiterhin strengen Voraussetzungen und bedarf zum Beispiel der vorherigen Einwilligung des Betroffenen. Das gilt in der Regel auch im Bereich des E-Mail-Marketings.





Vergleich von Datenschutzrichtlinie und EU-Grundverordnung zum Datenschutz

Im Folgenden finden Sie **elementare Bestandteile**, die grundlegend gleich geblieben sind sowie die wichtigsten Neuerungen:

Das ist geblieben

- Weiterhin muss in Unternehmen, deren Hauptaktivität die Datenerhebung und Datenverarbeitung oder die dauerhafte Beobachtung von Personen ist, laut EU-Datenschutzverordnung ein **betrieblicher Datenschutzbeauftragter** installiert sein.
- Die Weiterverarbeitung von Daten ist von der jeweiligen **Zweckbestimmung** abhängig. Erhobene personenbezogene Daten dürfen mithin nicht zweckentfremdet werden. Die jeweiligen Vorgänge müssen entsprechend transparent sein.



Vergleich von Datenschutzrichtlinie und EU-Grundverordnung zum Datenschutz

Im Folgenden finden Sie **elementare Bestandteile**, die grundlegend gleich geblieben sind sowie die wichtigsten Neuerungen:

Das hat sich im Wesentlichen verändert

- Der **Anwendungsbereich hat sich erweitert**: Mithin unterliegen auch Unternehmen und Anfragende aus Drittländern denselben Vorgaben wie die Mitgliedstaaten, sobald die Vorgänge EU-Bürger betreffen bzw. deren personenbezogene Daten.
- Die **Einwilligungshandlung** muss strengeren Vorgaben genügen (z. B. durch Kontrollkästchen auf Webseiten, Auswahl spezifischer Einstellungen usw.). Das stillschweigende Einverständnis genügt nicht mehr. Sind unterschiedliche Datenverarbeitungsvorgänge geplant, muss in jeden einzelnen gesondert eingewilligt werden können.



Vergleich von Datenschutzrichtlinie und EU-Grundverordnung zum Datenschutz

Im Folgenden finden Sie **elementare Bestandteile**, die grundlegend gleich geblieben sind sowie die wichtigsten Neuerungen:

Das hat sich im Wesentlichen verändert

- Die erteilte Einwilligung muss der Betroffene **jederzeit und unbegründet widerrufen** können. Der Widerruf muss einfach und verständlich möglich sein.
- Es muss dem Betroffenen möglich sein, aktiv gegen **einzelne Zwecke der Datenverarbeitung** – etwa dem Profiling oder Direktmarketing – zu widersprechen.
- Das bereits bestehende **Koppelungsverbot** wurde in der EU-Datenschutzgrundverordnung noch einmal verschärft: Ein Vertrag darf etwa nicht mehr davon abhängig gemacht werden, dass der Betroffene eine Einwilligung in die Datenverarbeitung erteilt.



Vergleich von Datenschutzrichtlinie und EU-Grundverordnung zum Datenschutz

Im Folgenden finden Sie **elementare Bestandteile**, die grundlegend gleich geblieben sind sowie die wichtigsten Neuerungen:

Das hat sich im Wesentlichen verändert

- Die **Auskunftsrechte der Betroffenen** wurden inhaltlich erweitert: Nunmehr sollen auch Angaben zu der jeweiligen Rechtsgrundlage der erhobenen und verarbeiteten Daten oder die Dauer der Speicherung bzw. der Kriterien genannt werden.
- Mit der neuen EU-Verordnung zum Datenschutz müssen Unternehmen ferner in der Lage sein, die von dem Betroffenen überlassenen Daten in einem **portablen und dennoch sicheren Format** an diesen oder – auf dessen Wunsch – direkt an einen Dritten auszuhändigen.



Vergleich von Datenschutzrichtlinie und EU-Grundverordnung zum Datenschutz

Im Folgenden finden Sie **elementare Bestandteile**, die grundlegend gleich geblieben sind sowie die wichtigsten Neuerungen:

Das hat sich im Wesentlichen verändert

- Die Pflicht zur **Löschung** veralteter oder falscher Daten wurde erweitert, sodass nunmehr die öffentlichen und nicht öffentlichen Stellen, die solche an Dritte weitergegeben haben, die jeweiligen Ansprechpartner kontaktieren und über die Unrichtigkeit in Kenntnis setzen müssen.
- Datenverarbeiter können bei Fehlern und Pannen vom Betroffenen mitunter auch direkt zur Verantwortung gezogen werden (**Schadensersatzansprüche** u. ä.).
- Es bedarf einer **regelmäßigen Risikobewertung** (Datenschutzfolgenabschätzung).



Vergleich von Datenschutzrichtlinie und EU-Grundverordnung zum Datenschutz

Im Folgenden finden Sie **elementare Bestandteile**, die grundlegend gleich geblieben sind sowie die wichtigsten Neuerungen:

Das hat sich im Wesentlichen verändert

- Die **Meldepflicht** im Falle einer Datenpanne wurde beschränkt auf einen Zeitraum von 72 Stunden, sobald die Rechte und Pflichten des Betroffenen durch die Panne einem Risiko ausgesetzt sind.
- Die **Geldbußen** im Falle eines Verstoßes gegen die in der EU-Datenschutzgrundverordnung festgehaltenen Grundsätze wurden noch weiter erhöht: auf bis zu 20 Millionen Euro oder 4 Prozent des weltweiten Umsatzes des Unternehmens (der höhere Wert entscheidet am Ende).



Linkliste

Gute Webseite für allgemeine Informationen zum Datenschutz mit Aktualisierungsnewsletter und Generator für Datenschutzerklärungen für Webseiten

<https://drschwenke.de>

Von der Universität Münster gibt es ebenfalls eine sehr gute Musterdatenschutzerklärung für Websitebetreiber nach den Vorgaben der DSGVO

<https://www.uni-muenster.de/Jura.itm/hoeren/lehre/materialien/musterdatenschutzerklaerung>

DSGVO Gesetz mit Verweis auf BDSG

<https://dsgvo-gesetz.de>

Bayerisches Landesamt für Datenschutzaufsicht (BayLDA – für nicht-öffentliche Stellen)

<https://www.lida.bayern.de/de/index.html>

Bayerischer Landesbeauftragter für Datenschutz (BayLfD – für öffentliche Stellen)

<https://www.datenschutz-bayern.de>



Linkliste

Offizielle Datenschutzseite der EU

https://ec.europa.eu/info/law/law-topic/data-protection_de

Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten
(auch Artikel-29-Datenschutzgruppe)

https://ec.europa.eu/info/law/law-topic/data-protection_en

Der Europäische Datenschutzausschuss ist gemäß Art. 94 Abs. 2 DSGVO der Nachfolger der sogenannten Artikel-29-Datenschutzgruppe, die auf Grundlage von Art. 29 der Datenschutz-Richtlinie 95/46/EG eingesetzt wurde.

https://edpb.europa.eu/edpb_de

Überprüfen Sie, ob die Verwendung von Cookies und Online-Tracking auf Ihrer Webseite die DSGVO und die ePrivacy Richtlinie (ePR) entspricht.

<https://www.cookiebot.com/de/>



Linkliste

Bayerisches Datenschutzgesetz – wirksam für öffentliche Stellen

<http://www.gesetze-bayern.de/Content/Document/BayDSG?AspxAutoDetectCookieSupport=1>

Webauftritt der Datenschutzkonferenz (DSK), dem Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder.

<https://www.datenschutzkonferenz-online.de>

Gute Informationen zu den verschiedensten Aspekten der DSGVO finden sich auch unter:

<https://www.datenschutzbeauftragter-info.de>