Bundesverband Deutscher Stiftungen

SKW Schwarz Rechtsanwälte

EU Datenschutz-Grundverordnung

RA Nikolaus Bertermann
Berlin, 7. März 2018

SKW
Schwarz
Rechtsanwälte

1. **Datenschutz Basics**
2. **Was ändert sich?**
3. **Datenschutzrechtlich relevante Prozesse in Stiftungen**
4. **Austausch und Diskussion**

- **Personenbezogene Daten**
  Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Abs. 1 DSGVO)

  Beispiele:

  – Mitarbeiterdaten (Stammdaten, Kontaktdaten, Bankverbindung, Personalakte; auch dienstliche Daten wie Telefonnummer oder dienstliche E-Mail-Adressen)
  – Daten von Zuwendungsempfängern, privaten Spendern, Teilnehmern an Veranstaltungen, Newsletterempfängern, ….
  – Partner und Lieferanten, bzw. Ansprechpartner bei Partnern und Lieferanten

- **Verantwortlicher** („Für die Verarbeitung Verantwortlicher“)
  Die natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

- **Dritter**
  Eine natürliche oder juristische Person, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

- **Kein Konzern- oder Verbund-Privileg**
  Auch die DSGVO kennt kein Konzern- oder Verbund-Privileg, d.h. verschiedene juristische Personen sind untereinander datenschutzrechtlich stets Dritte, egal ob ein Verbund oder eine rechtliche Beteiligung besteht.

SKW
Schwarz
Rechtsanwälte

Die Verarbeitung personenbezogener Daten ist nur zulässig, soweit die DS-GVO oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder die betroffene Person einwilligt.

Art. 6 DS-GVO, sog. „Verbot mit Erlaubnisvorbehalt“

- **Einwilligung**
  - jede freiwillig
  - für den bestimmten Fall,
  - in informierter Weise und
  - unmissverständlich
  - abgegebene Willensbekundung
  - in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung,

  mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

SKW
Schwarz
Rechtsanwälte

Gesetzlich erlaubt nach der DSGVO:

- Verarbeitung ist für die **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen **erforderlich**, die auf Anfrage der betroffenen Person erfolgen (Art. 6 Abs. 1 b) DSGVO)
- Verarbeitung ist zur **Erfüllung einer rechtlichen Verpflichtung erforderlich**, der der Verantwortliche unterliegt (Art. 6 Abs. 1 c) DSGVO)
- 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, … (Art. 6 Abs. 1 f) DSGVO)

- **Auftragsverarbeiter**
  Natürliche oder juristische Personen, die Daten im Auftrag des Verantwortlichen verarbeiten.

- Setzt den Abschluss eines gesonderten Vertrages mit Mindestinhalten voraus, die den bisherigen Anforderungen des § 11 BDSG im Wesentlichen entsprechen.

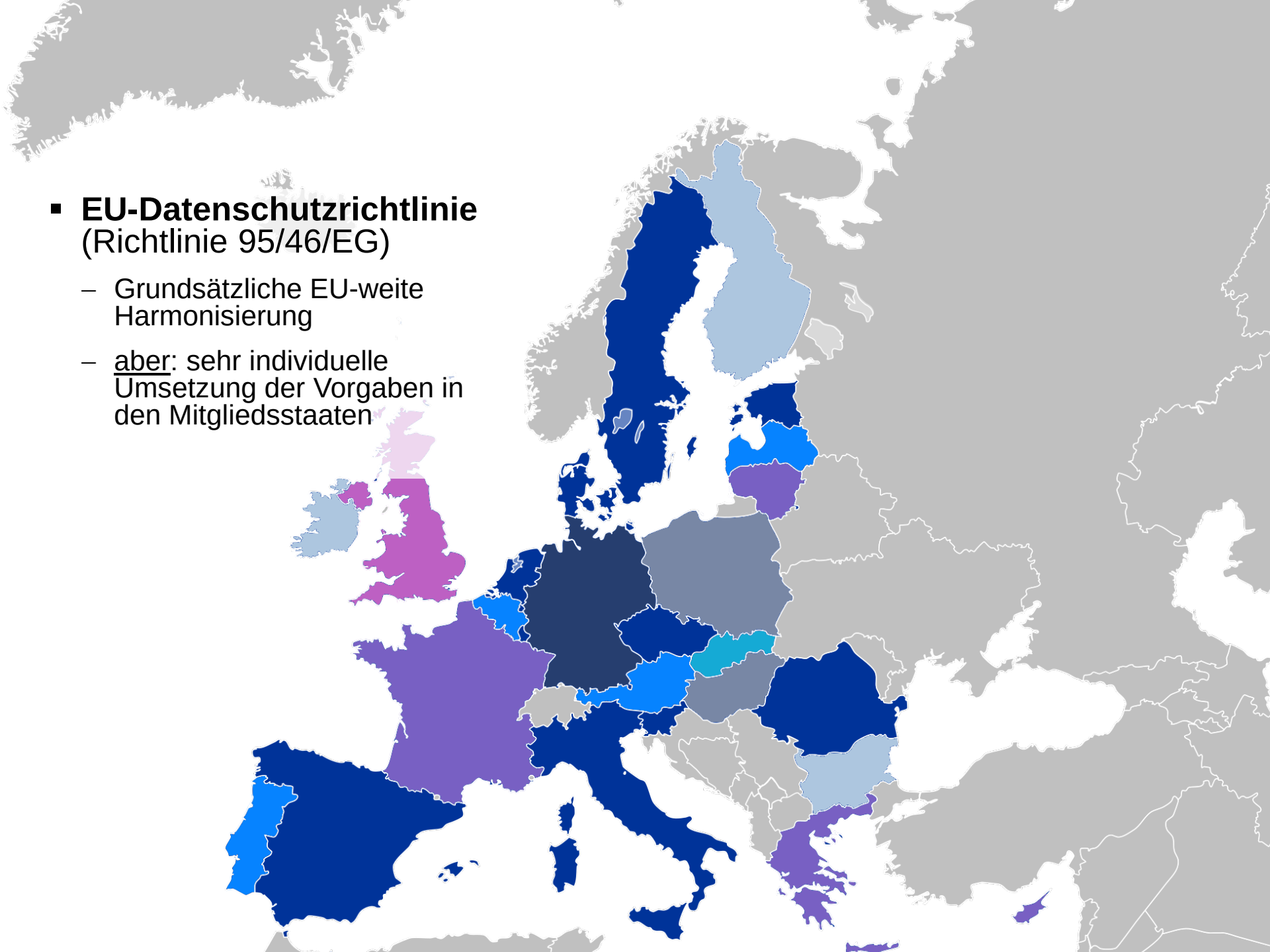
- Nach dem BDSG galten auch Wartungs- und Beratungsdienstleister als Auftragsdatenverarbeiter, wenn Ihnen personenbezogene Daten zur Kenntnis gelangt sind (§ 11 Abs. 5 BDSG).

- <u>Beispiele für Auftragsverarbeiter:</u>
  - Rechenzentrumsbetreiber, Hostprovider
  - Akten- und Datenvernichter
  - Archivierung
  - Call Center, Lettershops
  - Umfrageinstitute
  - ggf. verbundene Gesellschaften

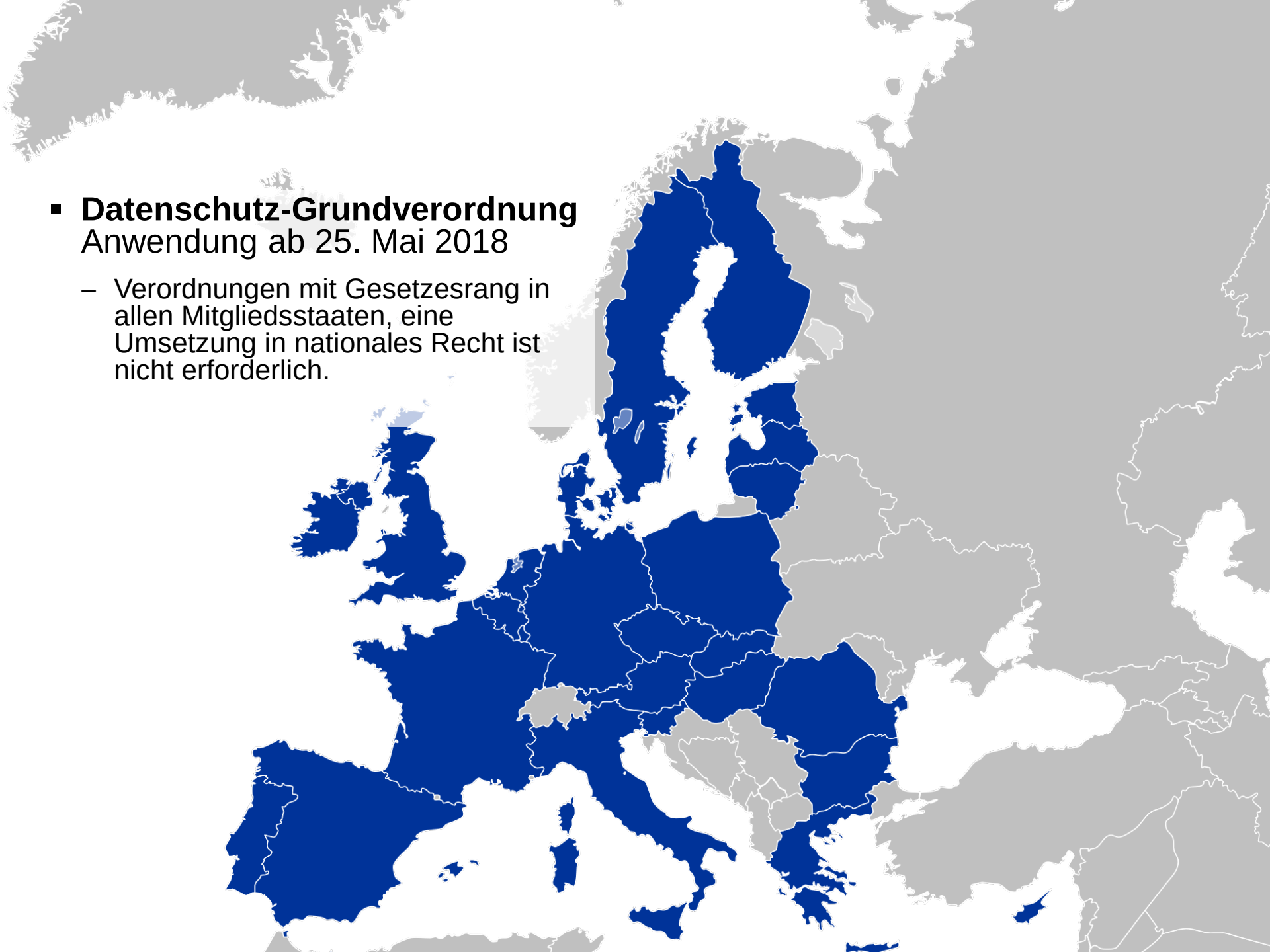
SKW
Schwarz
Rechtsanwälte

1. Datenschutz Basics
2. Was ändert sich?
3. Datenschutzrechtlich relevante Prozesse in Stiftungen
4. Austausch und Diskussion

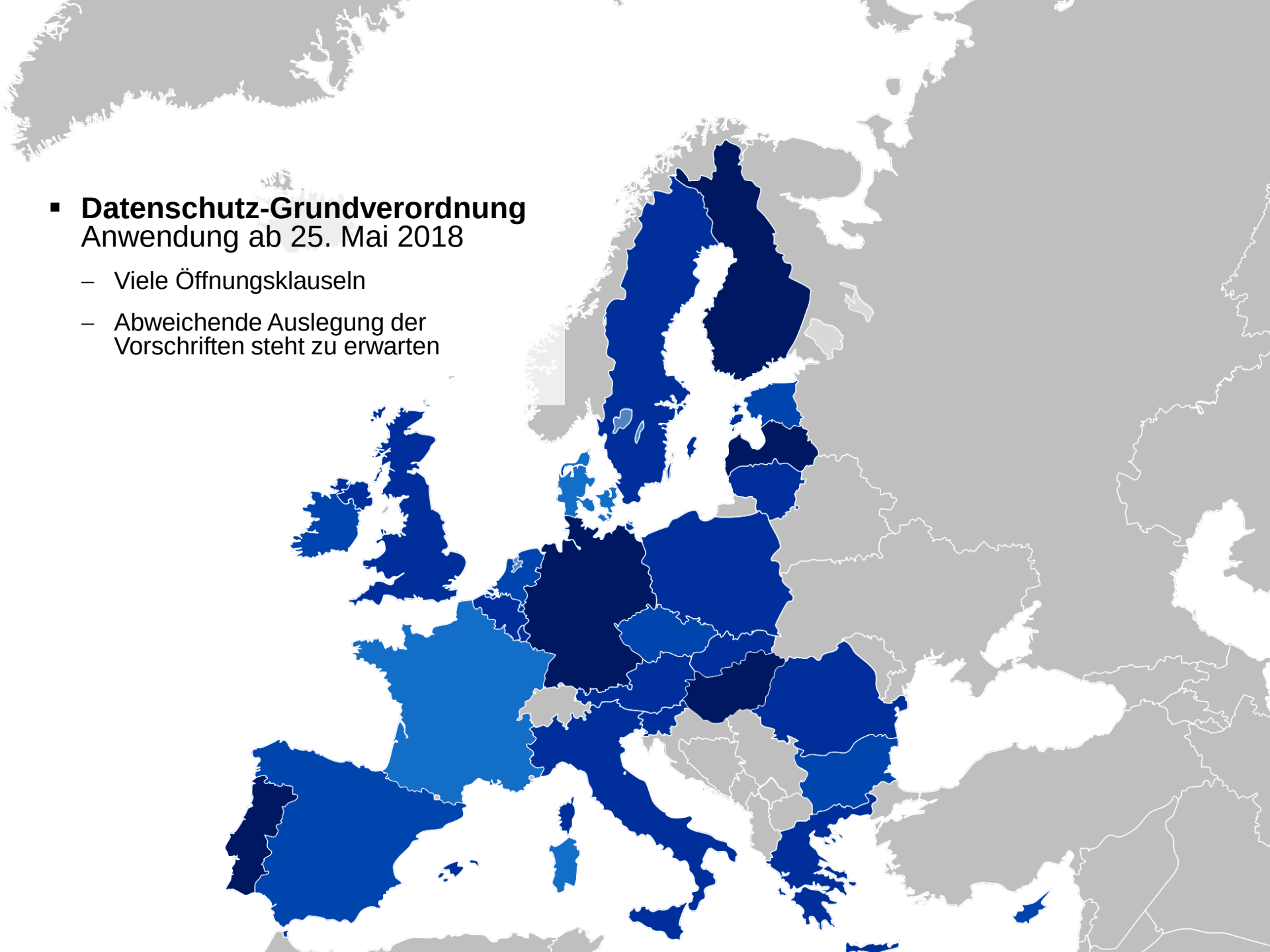
- **EU-Datenschutzrichtlinie** (Richtlinie 95/46/EG)
  - Grundsätzliche EU-weite Harmonisierung
  - aber: sehr individuelle Umsetzung der Vorgaben in den Mitgliedsstaaten



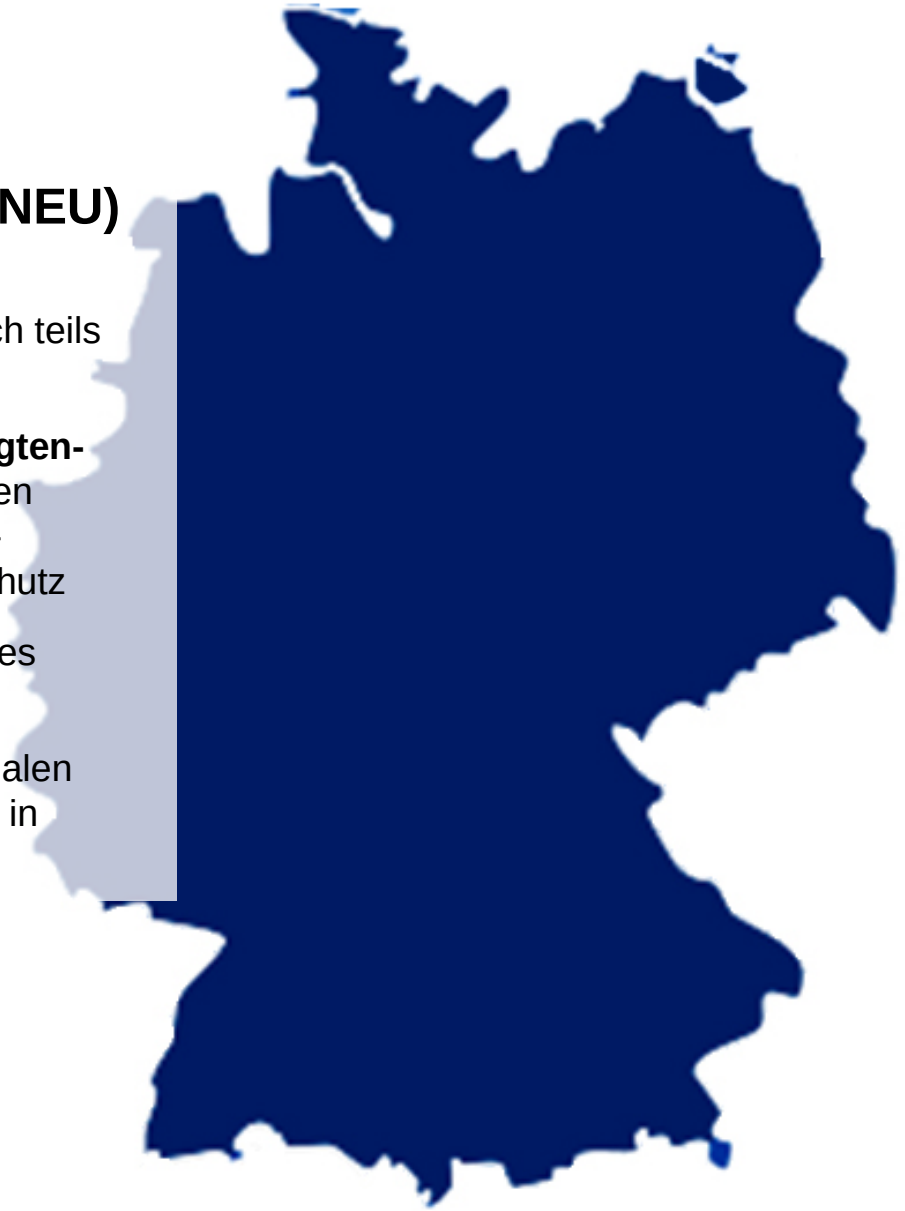
- **Datenschutz-Grundverordnung**
  Anwendung ab 25. Mai 2018
  - Verordnungen mit Gesetzesrang in allen Mitgliedsstaaten, eine Umsetzung in nationales Recht ist nicht erforderlich.



- **Datenschutz-Grundverordnung**
  Anwendung ab 25. Mai 2018
  - Viele Öffnungsklauseln
  - Abweichende Auslegung der Vorschriften steht zu erwarten



- **Bundesdatenschutzgesetz (NEU)**
  tritt ebenfalls zum 25.05.2018 in Kraft
  - Im Sommer 2017 beschlossen, vielfach teils heftige Kritik („europarechtswidrig!“)
  - Konkrete Regelungen zum **Beschäftigten-datenschutz** bleiben dicht am aktuellen § 32 BDSG und der bisherigen Recht-sprechung zum Beschäftigtendatenschutz
  - Fortführung der frühen Bestellpflicht des Datenschutzbeauftragten
  - Im Übrigen Regelungen zu den nationalen Aufsichtsbehörden und zur Vertretung in EU-Gremien



SKW
Schwarz
Rechtsanwälte

- Die DS-GVO enthält viele unbestimmte Rechtsbegriffe, deren konkrete Bedeutung in den kommenden Jahren erst durch die Fachliteratur, die deutschen und europäischen Aufsichtsbehörden und die nationalen Gerichte sowie den EuGH definiert und ausgelegt werden müssen.
- Das neue BDSG ist nach wie vor umstritten; ob es einer Prüfung durch den EuGH standhält ist aktuell zumindest teilweise fraglich.

→ Wir müssen vorerst mit einer gewissen **Rechtsunsicherheit** leben.

SKW
Schwarz
Rechtsanwälte

- **Übersicht der Verarbeitungstätigkeiten**

  Alle Datenverarbeitungen im Unternehmen müssen in einer strukturierten Datei nach den neuen Vorgaben der DS-GVO erfasst und dokumentiert werden.

- Personenbezogene Daten müssen **gelöscht** werden, wenn sie für die Zwecke, für die sie erhoben oder verarbeitet wurden, nicht mehr notwendig sind.

- Eine genauere Prüfung der Löschroutinen und der Vorgaben für die Löschung muss erfolgen.
- Die DS-GVO nennt die bisher in § 35 Abs. 3 Nr. 3 BDSG vorgesehene Sperrung von Daten, d.h. die faktische Zugriffssperrung auf Daten, nicht mehr ausdrücklich. Es ist umstritten, ob sich ein Recht des Verantwortlichen zur Sperrung im Wege der Interessenabwägung auch nach der DS-GVO herleiten lässt.

→ **Die Wirksamkeit und Angemessenheit der Löschroutinen muss überprüft werden, ggf. ist ein neues ganzheitliches Löschkonzept zu erstellen und umzusetzen.**

- **Informationspflichten**
  Die DS-GVO enthält umfangreiche Informationspflichten, die gegenüber Betroffenen erfüllt werden müssen (Art. 12-14 DS-GVO).

- Dies betrifft alle Datenverarbeitungen, sowohl gegenüber Mitarbeitern, Förderern, Leistungsempfänger, aber auch gegenüber Ansprechpartnern bei Lieferanten und Partnern. Es müssen geeignete Prozesse zur Information (Webseite, E-Mail, Formulare) eingeführt werden.

- <u>Beispiele für Pflichtinformationen:</u>
  - Art der Daten und Zweck der Verarbeitung
  - Rechtsgrundlage der Verarbeitung
  - Falls die Rechtsgrundlage „berechtigtes Interesse“ des Verantwortlichen ist, eine kurze Darstellung der vorgenommenen Interessenabwägung
  - Sämtliche Empfänger von Daten (inklusive der Auftragsverarbeiter)
  - Speicherdauer der Daten
  - Hinweise auf die Rechte des Betroffenen (z.B. Auskunft, Löschung, …)
  - Die Quelle der Daten (falls nicht direkt erhoben)
  - …

- Werden die Angaben zur Erfüllung der Informationspflichten nach den bereits in der Verarbeitungsübersicht erfasst, können die pro Verarbeitung bestehenden Informationspflichten aus der Übersicht extrahiert und konsolidiert werden.

- Im Anschluss kann die Umsetzung der Informationspflichten je Daten-Eingangskanal erfolgen (z.B. in der Datenschutzerklärung oder auf der Rückseite von Print-Formularen oder in E-Mail-Bestätigungen)

- Im Rahmen der Unterstützungspflicht in Art. 28 (Auftragsverarbeitung) kann es erforderlich sein, Kunden bei der Erstellung der Angaben für die Informationspflichten zu unterstützen, d.h. Musterdokumente für Kunden vorzuhalten.

- **Technische und organisatorische Maßnahmen**
  Es müssen unter Berücksichtigung u.a. des **Stand der Technik**, der **Eintrittswahrscheinlichkeit**, der **Schwere des Risikos** und der **Kosten** angemessene Maßnahmen zum Schutz der Daten getroffen werden.

- Die Maßnahmen müssen dokumentiert und nachweisbar sein. Sie müssen außerdem regelmäßig auf Funktionalität und Angemessenheit hin überprüft werden.

SKW
Schwarz
Rechtsanwälte

- **Was ist „Stand der Technik“?**

- Definition des „Stand der Technik“ / „State of the art“ ist nicht ganz klar – weder in Deutschland, noch innerhalb der EU.

- Einhaltung anerkannter Standards (z.B. ISO 27001, BSI Grundschutz) kann Indiz für den Stand der Technik sein.

- Festlegung muss nicht extern erfolgen, eigene Fachkunde im Unternehmen kann ebenfalls genutzt werden. Wichtig ist Dokumentation.

- Schutzziele nach der DS-GVO sind:
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit / Belastbarkeit
- Angemessene Maßnahmen unter Einbeziehung von:
  - Stand der Technik
  - Implementierungskosten
  - Art, Umfang, Umstände,
    Zwecke der Verarbeitung

- Zu berücksichtigende Schadenstypen:
  - physische Schäden
  - materielle Schäden
  - immaterielle Schäden
  - erhebliche wirtschaftliche Nachteile
  - erhebliche gesellschaftlichen Nachteile
- Identifikation relevanter Bedrohungen:
  - Bruch der Vertraulichkeit (intern, extern)
  - Verbreitung, Veröffentlichung
  - Veränderung, Löschung
  - Verlust
  - Nicht-Verfügbarkeit
- Ermittlung der Risikoklasse; ggf. Reduzierung des Risikos durch geeignete technische und organisatorische Maßnahmen

SKW
Schwarz
Rechtsanwälte

- **Pflicht zur Verschwiegenheit**
  Mitarbeiter dürfen personenbezogene Daten nur für die konkret festgelegten Zwecke verarbeiten und müssen die Daten vertraulich behandeln.

- **Verpflichtung auf Vertraulichkeit**
  Wir schon nach dem BDSG („Datengeheimnis“) bedarf es auch nach der DS-GVO einer Verpflichtung aller Mitarbeiter auf die Vertraulichkeit.

- Es müssen alle Verträge mit eigenen Auftragsverarbeitern an die Anforderungen der DS-GVO anpassen.

- Zwischen verbundenen Gesellschaften kann ggf. eine (Rahmen-) Vereinbarungen zur Auftragsverarbeitung abgeschlossen werden.

SKW
Schwarz
Rechtsanwälte

- **Datenschutz-Folgenabschätzung**

  Für jede Datenverarbeitung muss zunächst eine einfache Risiko-Analyse durchgeführt werden. Nach dieser definiert sich auch die Schutzklasse.

- Ergibt sich aus der Analyse ein **hohes Risiko** für die Rechte der Betroffenen, so ist eine förmliche Datenschutz-Folgenabschätzung (DSFA) durchzuführen und deren Ergebnis ist zu dokumentieren.

- Die konkreten Voraussetzungen sind noch umstritten, auch unter den deutschen Aufsichtsbehörden. Es steht aber zu erwarten, dass bei sensiblen Personaldaten eine DSFA durchzuführen ist. Es muss voraussichtlich für die Teile der Personaldatenverarbeitung und für Videoüberwachungen eine DSFA durchführen und wird voraussichtlich auch von Kunden um Unterstützung gebeten werden.

- Die DS-GVO verpflichtet zu „Privacy-by-design“, d.h. zu datenschutzfreundlicher Technikgestaltung und -entwicklung.
- Außerdem verlangt die DS-GVO „Privcy-by-default“; Software und Services müssen so eingestellt sein, dass möglichst wenig Daten verarbeitet werden.

- Die DS-GVO verpflichtet zur Meldung von Datenschutzverstößen an die Aufsichtsbehörde binnen 72 Stunden. Die Regelung ist weitreichender als nach dem BDSG.

→ **Es muss einen entsprechender Meldeprozess eingeführt und dokumentiert werden.**

- **Auskunftspflicht**
  Die DS-GVO enthält Auskunftspflicht (wie schon das BDSG).

- Auskunft zu sämtlichen zu einer Person gespeicherten Daten muss auf Wunsch des Betroffenen in Papier- oder Textform erteilt werden. Ein entsprechender Prozess muss gestalten werden. Auch Kunden werden Zugriff auf diesen Prozess benötigen.

- **Recht auf Kopie der gespeicherten Daten**
  Das Auskunftsrecht umfasst automatisch einen Anspruch auf eine Kopie aller gespeicherten Daten!

- **Recht auf Datenübertragbarkeit**
  Bei Daten, die auf Grundlage eines Vertrages oder einer Einwilligung verarbeitet werden, besteht ein Anspruch darauf, dass die Daten in einem strukturierten, gängigen und maschinenlesbaren Format auf Verlangen des Betroffenen an einen Dritten übertragen werden.

- **Weitere Betroffenenrechte**
  Die DS-GVO enthält weitere, inhaltlich teilweise veränderte und erweiterte Rechte der Betroffenen, wie:
  - Widerspruchsrecht bei Interessenabwägung
  - Berichtigungsanspruch
  - Löschanspruch
  - Anspruch auf Einschränkung der Verarbeitung

→ **Bestehende Prozesse müssen an die neuen Anforderungen angepasst werden; soweit Prozesse nicht dokumentiert sind, muss eine Dokumentation erfolgen.**

- **Rechenschaftspflicht („Accountabiity“)**
  - Die DS-GVO verlangt von jedem Verantwortlichen einen „Nachweis“, dass die Vorgaben der DS-GVO eingehalten werden.
  - Die englische Sprachfassung spricht „nur“ von „to demonstrate“ (im Deutschen eher „aufzeigen“, „glaubhaft zeigen“).

→ **Es muss eine interne Dokumentation erstellt werden, die den „Nachweis“ der Einhaltung der DS-GVO erbringt.**

SKW
Schwarz
Rechtsanwälte

- **Bußgelder und Strafen**
  - DS-GVO ausdrücklich nur gegen den „Verantwortlichen“ vorgesehen, das BDSG-neu erlaubt aber auch (weiter) Bußgelder gegen handelnde Personen (Mitarbeiter).

- **Bußgeldhöhe bisher (BDSG)**
  - bis 50.000 EUR bei weniger schwerwiegenden Verstößen
  - Bis 300.000 EUR bei schwerwiegenden Verstößen

- **Bußgeldhöhe ab 25.05.2018 (DSGVO)**
  - bis 10 Mio€ oder 2% des Jahresumsatzes bei weniger schwerwiegenden Verstößen
  - Bis 20 Mio€ oder 4% des Jahresumsatzes bei schwerwiegenden Verstößen

SKW
Schwarz
Rechtsanwälte

1. Datenschutz Basics
2. Was ändert sich?
3. Datenschutzrechtlich relevante Prozesse in Stiftungen
4. Austausch und Diskussion

- Juristische Personen des Privatrechts
- Stiftungen des öffentlichen Rechts
- Nicht rechtsfähige Stiftungen
- Kirchliche Stiftungen

SKW
Schwarz
Rechtsanwälte

- Der Transfer von personenbezogenen Daten zwischen einer Stiftung und ihren Veranstaltungs-GmbHs oder ähnlichen Gesellschaften bedarf einer Rechtsgrundlage!

SKW
Schwarz
Rechtsanwälte

- Verwaltung von Spenderdaten und anderen Kontakten muss strukturiert und organisiert sein
- Die DS-GVO gilt auch für strukturierte Papierarchive

SKW
Schwarz
Rechtsanwälte

- Das KUG ist ab 25.05.2018 nicht länger Spezialgesetz, d.h. die DS-GVO geht dem KUG vor. Damit sind Einwilligungen in die Veröffentlichung von Lichtbildern jederzeit widerrufbar.
- Ein Ausschluss des Widerrufsrechts wäre mit der DS-GVO nicht zu vereinbaren; einzige Lösungsmöglichkeit schein eine klare Information und bspw. die Einwilligung in eine konkrete (Druck-) Auflage.

SKW
Schwarz
Rechtsanwälte

1. **Datenschutz Basics**
2. **Was ändert sich?**
3. **Datenschutzrechtlich relevante Prozesse in Stiftungen**
4. **Austausch und Diskussion**

SKW Schwarz Rechtsanwälte
Neues Kranzler Eck
Kurfürstendamm 21
10719 Berlin

Rechtsanwalt
Nikolaus Bertermann
zertifizierter Datenschutzauditor (TÜV)
Fachanwalt für Informationstechnologierecht

Tel: 030 / 889 26 50 45
Fax: 030 / 889 26 50 10
Mail: n.bertermann@skwschwarz.de
Web: www.skwschwarz.de