Die EU-Datenschutzgrundverordnung und das neue Bundesdatenschutzgesetz

Die EU-Datenschutzgrundverordnung (EU-DSGVO) gilt nun **unmittelbar und zwingend!** Es bedarf keiner Umsetzung mehr.

Am **25.05.2018** gilt die Verordnung mit ihren 172 Erwägungsgründen und den 99 Artikeln. Es gibt keine weitere Übergangsfrist.

Grundsätzliches

- Umsetzung der Richtlinie hat nicht funktioniert.
- Irland, Großbritannien etc. haben „Sanktionen“ weggelassen.
- Internetkonzerne (z. B. Facebook etc.) haben Hauptsitz verlegt.

- Zweck: Harmonisierung des europäischen Datenschutzes.
- Gleiches Datenschutzniveau soll in Europa herrschen.

- Nationale „Öffnungsklauseln“ möglich.
- Jedoch keine Lockerung des Datenschutzes.
- Hat der deutsche Gesetzgeber genutzt:
- Am 25.05.18 tritt ebenfalls das neue Bundesdatenschutzgesetz in Kraft, welches das bisherige BDSG ablöst.

Natürliche Personen
Art. 1 DSGVO

Personenbezogene Daten
Art. 4 Ziffer 1 DSGVO

- Was ist geschützt? – die personenbezogenen Daten von **natürlichen Personen** (Art. 1 EU-DSGVO).
- Was genau sind **„personenbezogene Daten“**? Alle Informationen von/über eine natürliche Person („Betroffener“ oder auch „betroffene Person“).
- Es genügt die Identifizierbarkeit (Art. 4 Ziffer 1 EU-DSGVO).
- Mitgliedsnummern im Verein ist hierfür ausreichend.

„Verarbeiten“

Art. 4 Ziffer 2 DSGVO

Bei welchen Handlungen greift nun der Datenschutz? – Die EU-DSGVO spricht nur noch von dem Oberbegriff „Verarbeiten“

Danach ist verarbeiten (automatisiert und auch nicht automatisiert)

Erheben	**Das Auslesen**
Erfassen	**Das Abfragen**
Die Organisation	**Die Verwendung**
Das Ordnen	**Die Offenlegung durch Übermittlung**
Die Speicherung	**Verbreitung**
Die Anpassung	**Andere Form der Bereitstellung**
Veränderung	**Abgleich**
Verknüpfung	**Einschränkung**
Löschung	**Vernichtung**

Verantwortlicher

Art. 4 Nr. 7 DSGVO

- Jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder mit anderen gemeinsam über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

- Derjenige, der also diese personenbezogenen Daten – nicht für die private Verwendung – verarbeitet und die Zwecke hierfür definiert ist **Verantwortlicher!**

Auftragsverarbeiter

Art. 4 Nr. 8 DSGVO

- Natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten **im Auftrag** des Verantwortlichen verarbeiten.
- Nach h.M. Fortgeltung der Weisung als wichtigste Voraussetzung

Grundsätze der Verarbeitung

Art. 5 DSGVO

- Rechtmäßigkeit der Verarbeitung
- Verarbeitung nach Treu- und Glauben
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit – die personenbezogenen Daten müssen richtig und auf dem neuesten Stand sein.
- Speicherbegrenzung (nur solange für die Durchführung des Zwecks erforderlich ist)
- Integrität und Vertraulichkeit – Gewährleistung einer angemessenen Sicherheit durch **technische und organisatorische Maßnahmen**.
- Rechenschaftspflicht – Verantwortung des Verantwortlichen und Nachweis der Einhaltung der vorgenannten Grundsätze (Dokumentation!)

Rechtmäßigkeit der Verarbeitung

Art. 6 DSGVO

- „Verarbeitung“ von personenbezogene Daten nur erlaubt, wenn dieses durch gesetzliche Vorschrift oder durch Einwilligung gedeckt ist. → Verbotsnorm mit Erlaubnisvorbehalt.

- Achtung:

Informationspflichten in Art. 13 und 14. sehen vor, dass Anspruchsgrundlage genannt wird.

Zulässigkeits-tatbestände nach
Art. 6 DSGVO

- Einwilligung (Art. 7 und 8 EU-DSGVO)
- Zur Erfüllung eines Vertrages sowie auch vorvertragliche Maßnahmen → Erforderlichkeit notwendig
- Rechtliche Verpflichtung → d.h., wenn eine andere Norm (auch zivilrechtliche Norm) dieses erlaubt (so z.B. die Dokumentationspflichten nach dem MiLoG).
- [...]

Zentrale Norm

Art. 6 Abs. 1, S. 1, **f** DSGVO

- Die **zentrale Norm** wonach *die Verarbeitung zur Wahrung des berechtigten Interesses des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen (insbesondere Kinder).*
- z.B. Verarbeitung personenbezogener Daten zu Zwecken der Direktwerbung.
- Spielraum für mögliche Nutzungsvarianten.
- Gedanken zwingend dokumentieren und bei der Zweckbeschreibung rechtzeitig berücksichtigen.
- **Diese Norm ist auch für die Videoüberwachung einschlägig – Konkretisierung im neuen BDSG**

Informationspflichten
Art. 13 und 14 DSGVO

- Es wird zwischen der Direkterhebung beim Betroffen (Art. 13) und der indirekten Erhebung aus anderen Quellen (Internet, Adresshändler -> Art. 14 DSGVO) differenziert:

  - Verantwortlicher und Vertreter
  - Nennung des Datenschutzbeauftragten
  - Zwecke und Rechtsgrundlage der Verarbeitung
  - Datenkategorien (nur Art. 14)
  - Berechtigte Interessen
  - Empfänger oder Kategorien von Empfängern
  - Drittstaatstransfer (außerhalb der EU)
  - Speicherdauer

Informationspflichten

Art. 13 und 14 DSGVO

- Mitteilung der Rechte des Betroffenen (Auskunftsanspruch, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch, Datenübertragbarkeit).
- Hinweis auf die Widerrufsmöglichkeit der Einwilligung
- Beschwerderecht
- Pflicht zur Bereitstellung der Daten (nur Art. 13 – Direkterhebung)
- Datenquellen (Auskunft, woher die Daten stammen – Nur Art. 14 – indirekte Erhebung).
- Ggf. automatisierte Entscheidungsfindung (z.B. bei Scoring etc.).

Löschen personenbezogener Daten

Art. 17 Abs. 1 DSGVO

- Für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind
- Die betroffene Person ihre Einwilligung widerruft und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt
- Die betroffene Person Widerspruch gegen die Verarbeitung einlegt und keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen
- Die personenbezogenen Daten unrechtmäßig verarbeitet wurden
- [...]

Löschen von Links

- Es sind auch die Links im Falle einer Veröffentlichung im Internet zu löschen. Es sollte somit zumindest geprüft werden, wie die Daten auch z.B. von Google gelöscht werden können.
- Im Zweifel sind die Suchmaschinenbetreiber standardisiert anzuschreiben, um das Löschungsbegehren des Betroffenen auch dort weiter zu geben. (Recht auf „Vergessenwerden“).
- Der Betroffene ist spätestens innerhalb 1 Monats über sein Löschungsbegehren und dessen Umsetzung oder Ablehnung zu informieren.

Ausnahmen zur Löschungspflicht

- soweit die Verarbeitung erforderlich ist
- bei Ausübung des Rechts auf freie Meinungsäußerung und Information
- [...]
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Schutz durch Technikgestaltung

Art. 25 DSGVO

- Datenminimierung
- Ggf. Pseudonymisierung
- Transparenz in Bezug auf Funktion und Verarbeitung
- Ermöglichung der Überwachung der Verarbeitung durch die betroffene Person
- Ggf. Ermöglichung für Sicherheitsfunktionen „on top“ durch Verantwortlichen
- Dabei sind die Regelungen gerade nicht starr, sondern orientieren sich an dem jeweiligen „Stand der Technik“ und dem Möglichen (Abwägung zu den Implementierungskosten – Wirtschaftlichkeit einer Maßnahme und Aufwand)

Das neue Bundesdatenschutz-gesetz (BDSG)

- Das BDSG neu tritt ebenfalls am 25.05.2018 in Kraft und wird bisher bestehende BDSG vollständig ablösen.
- Da die EU-DSGVO nun eine Verordnung ist und für alle EU-Länder unmittelbar und zwingend gilt, darf der deutsche Gesetzgeber mit dem neuen BDSG nicht von der DSGVO abweichen.
- Er darf lediglich **konkretisieren.** Gleichwohl hat der deutsche Gesetzgeber versucht, auch noch seine eigenen Regelungen bestehen zu lassen. Ob dieses so Bestand haben wird, muss sich noch zeigen.

Die wichtigsten Änderungen

- Sonderregelungen: Das Gesetz enthält Sonderregelungen zu einigen Spezialgebieten, wie etwa dem Datenschutz am Arbeitsplatz, Videoüberwachung oder Profiling.
- Erschwerte Compliance-Kontrollen: Die Aufklärung von Straftaten oder anderen Pflichtverstößen bleibt zulässig, muss aber strengen Anforderungen genügen – gerade bei der Transparenz der Datenverarbeitung.
- Transparenz: Es bleibt weitgehend bei den umfassenden Unterrichtungspflichten nach Art. 13 ff. DSGVO. Eine Ausnahme gilt im Endeffekt nur für Notsituationen oder bei strafbaren Handlungen.

Datenschutz-beauftragter

§ 38 BDSG

- Jedes Unternehmen, das mehr als 10 Mitarbeiter beschäftigt, die einen Computerarbeitsplatz haben, muss einen Datenschutzbeauftragten bestellen.
- Werden besondere personenbezogene Daten verarbeitet, die eine Datenschutzfolgeabschätzung nach Art. 35 EU-DSGVO erfordern oder zu Geschäftszwecken zur weiteren Übermittlung oder der Markt- und Meinungsforschung haben diese Unternehmen unabhängig von der Anzahl der Beschäftigten einen Datenschutzbeauftragten zu bestellen.

Haftungsregelungen

- Beschwerderecht des Betroffenen - nach Art. 77 EU-DSGVO
- Schadensersatz gegenüber dem Verantwortlichen oder Auftragsverarbeiter – nach Art. 79 EU-DSGVO

Haftung und Recht auf Schadensersatz

Art. 82 DSGVO

- Schadensersatz nur bei rechtswidrigem Handeln des Verarbeiters bzw. des Auftragsverarbeiters und ein Verschulden gem. § 276 BGB (Vorsatz oder Fahrlässigkeit).
- Gem. Art. 82 Abs. 3 EU-DSGVO ist auch noch eine Beweislastumkehr vorgesehen.

Geldbußen
Art. 83 DSGVO

- Nach Art. 83 Abs. 1 EU-DSGVO soll jede Aufsichtsbehörde sicherstellen, dass Geldbußen bei Verstößen gegen diese Verordnung in jedem Einzelfall **wirksam, verhältnismäßig und abschreckend** sind.
- Daraus wird allgemein gefolgert, dass die Bußgelder nun doch deutlich teurer werden, als dieses bisher unter dem Regime der Datenschutzrichtlinie sowie des alten BDSG der Fall war.

Bußgeldrahmen
Art. 83 Abs. 4 DSGVO

- Bei geringeren Verstößen gilt ein Bußgeldrahmen von bis zu 10 Mio. € oder (bei Unternehmen) bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes – maßgeblich ist der höhere Betrag.
- Dies gilt z.B. bei
  - Verstößen gegen die Einwilligung eines Kindes
  - Verstöße bei der Verarbeitung von personenbezogenen Daten, für die eine Identifizierung des Betroffenen nichterforderlich bzw. nur mit der Speicherung von weiteren Informationen möglich ist (z.B.: Speicherung von Telefondaten / Zielrufnummern – Hier ist derjenige, dem diese Rufnummer gehört nicht gesondert zu informieren).
  - Verstoß gegen datenschutzfreundliche Voreinstellungen in der Software

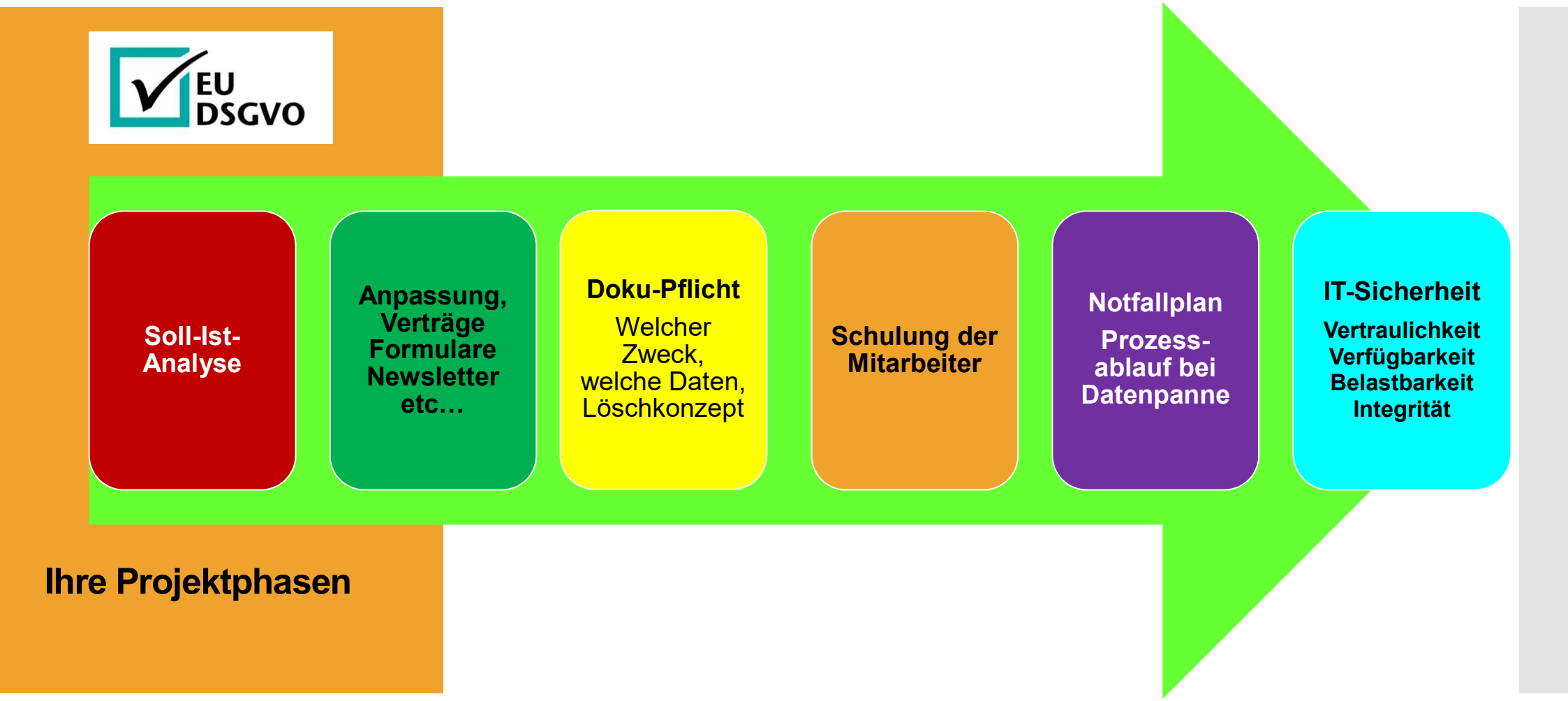
Bußgeldrahmen
Art. 83 Abs. 5 DSGVO

- Gem. Art. 83 Abs. 5 EU-DSGVO können Geldbußen bis zu 20 Mio. € oder im Falle eines Unternehmens bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden, bei

  - Verstößen gegen die Einwilligung
  - Verstöße gegen Informationspflichten.
  - Verstößen bei der Übermittlung in ein Drittland
  - Nichtbefolgung einer Anweisung der Datenschutzbehörde

Zivilrechtliche und strafrechtliche Betrachtung

- Verschärfte Haftung des Datenschutzbeauftragten: Größere Schwierigkeiten einen „Internen“ zu finden. Vollständige Kontrollfunktion - nunmehr sowohl eine zivilrechtliche als auch eine echte strafrechtliche Haftung des Datenschutzbeauftragten durch Unterlassen möglich ist.
- Zudem haben wir im BDSG neu in § 83 Abs. 1 BDSG die Haftung des Verantwortlichen oder des Rechtsträgers. Das bedeutet, dass der Geschäftsführer einer juristischen Person (z.B. GmbH) auch haften kann und ebenfalls in Anspruch genommen werden könnte und nicht die juristische Person selbst.


EU DSGVO
Soll-Ist-Analyse
Anpassung, Verträge Formulare Newsletter etc…
Doku-Pflicht
Welcher Zweck, welche Daten, Löschkonzept
Schulung der Mitarbeiter
Notfallplan
Prozess-ablauf bei Datenpanne
IT-Sicherheit
Vertraulichkeit
Verfügbarkeit
Belastbarkeit
Integrität
Ihre Projektphasen

Projektstart
Umsetzungstipps
Checklisten

- Der Kommunikationsphase (Analyse der neuen Anforderungen und des Änderungsbedarfs – Kommunikation des Änderungsbedarfs)
- Erstellung eines Aktionsplans (mittels soll – ist – Abgleich)
- Umsetzungsphase (Anpassung der Verträge, Meldungen, internen Prozesse, Betriebsvereinbarungen etc.)
  - Nachweis- / Dokumentationspflichten aufgrund der Accountability
  - Aktualisierung der Schulung der Mitarbeiter
  - Etablierung des Prozesses der „Datenschutzfolgenabschätzung“
  - Etablierung eines Prozesses bei Datenpannen
  - Umsetzung der antragsunabhängigen Verpflichtung zur Löschung

Projektstart
Umsetzungstipps
Checklisten

- Gewährleistung der Betroffenenrechte (Auskunft, Löschung, Berichtigung, Widerspruch, Vergessenwerden, Datenportabilität)
- Überprüfung der IT-Sicherheit: Vertraulichkeit, Integrität und Verfügbarkeit plus Belastbarkeit. Dokumentationspflicht, um den Nachweis der Konformität zu führen.
- Überprüfung der eigenen zur Verfügung gestellten Software: Berücksichtigung von Privacy–by–Design und Privacy–by– Default (geeignete technische und organisatorische Maßnahmen zur Umsetzung der Datenschutzgrundsätze in der Software sowie geeignete technische und organisatorische Maßnahmen, um durch Voreinstellungen sicherzustellen, dass nur zweckbestimmte personenbezogene Daten verarbeitet werden).

Projektstart
Umsetzungstipps
Checklisten

- Transparenzpflichten und Betroffenenkommunikation (weitgehende Informationspflichten): Die Informationen sollen in leicht zugänglicher und verständlicher sowie klarer und einfacher Sprache abgefasst sein. Aus Erwägungsgrund 58 ergibt sich, dass diese Informationen auch in elektronischer Form zur Verfügung gestellt werden können.

- Prüfung des Einwilligungsmanagements (laut Beschluss des Düsseldorfer Kreises sollen einmal unter dem Regime des BDSG erteilte wirksame Einwilligungen ihre Wirksamkeit behalten, so dass es keiner neuen Einwilligungen bedarf).

- Anpassung der Verträge – insbesondere mit Auftragsverarbeitern.

Häufige Fragen

- Betreibergesellschaft ist Auftragsverarbeiter des Golfclubs
- Buchung von Startzeiten/Turnieren für weitere Mitspieler
- Beweispflicht bei der Beschwerde eines Mitglieds
- Legitimation der Mitglieder bei der Bestellung von DGV-Ausweisen
- Habe über DGV-Intranet Zugriff auf persönliche Daten (Geburtstag). Ist das zulässig?
- Beispiele für Bußgelder im Betrieb von Golfanlagen

Lösungen für Mitglieder

des Golfverbandes Rheinland-Pfalz, Saarland e.V.

A) Projektleiter

- ✓ Überprüfung Ist-Zustands
- ✓ Vorlage Musterverzeichnis für Verarbeitungstätigkeiten
- ✓ Empfehlung / Verbesserungsvorschläge
- ✓ Beratung per Telefon und Email

Einmalzahlung: € 1.500,-

+ Monatlich € 150,-

B) Projektleiter & Datenschutzbeauftragter

Paket A plus zusätzlich:

- ✓ DSB-Haftung bis zu 1,5 Mio € pro Versicherungsfall
- ✓ Schulung der Mitarbeiter
- ✓ Notfallkonzept
- ✓ Einmal jährliche Kontrolle

Einmalzahlung: € 2.500,-

+ Monatlich € 250,00

C) Premium

Paket A+B plus zusätzlich

- ✓ Kommunikation mit Auskunftsbegehren und Datenschutzbehörden
- ✓ Erstellung des Verzeichnisses der Verarbeitungstätigkeiten
- ✓ 24/7 Support bei Datenschutzpannen

Einmalzahlung: € 3.500,-

Monatlich € 350,-

elblaw
RECHTSANWÄLTE

elblaw
Rechtsanwälte

Vielen Dank für Ihre Aufmerksamkeit.

Karsten Klug
Rechtsanwalt
Fachanwalt für Arbeitsrecht
Externer Datenschutzbeauftragter (TÜV).

Haben Sie noch weitere Fragen?

Tel.: 040 / 411 89 38 – 28
Fax: 040 / 411 89 38 – 37
Mail: klug@elblaw.de