Datenschutz im Verein

9. Fachtag für bürgerschaftliches Engagement im ländlichen Raum

Coswig, 14.09.2018

Vereins- und Stiftungszentrum
www.vereine-stiftungen.de

Anlass

- Inkrafttreten der Datenschutzgrundverordnung (DSGVO) nebst Novelle Bundesdatenschutzgesetz (BDSG 2018) zum 25.05.2018
- ersetzt bisheriges Datenschutzrecht

Vereins- und Stiftungszentrum
www.vereine-stiftungen.de

Sachlicher Anwendungsbereich

- automatisierte und nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen
- Dateisystem = jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich ist

Vereins- und Stiftungszentrum
www.vereine-stiftungen.de

Persönlicher Anwendungsbereich

- gilt für jeden, der in der EU personenbezogen Daten verarbeitet oder außerhalb der EU personenbezogene Daten von EU-Bürgern verarbeitet
- gilt nicht für die Verarbeitung zu persönlichen oder familiären Zwecken durch natürliche Personen

Vereins- und Stiftungszentrum
www.vereine-stiftungen.de

Personenbezogene Daten

- alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen

→ „Betroffener“ oder „betroffene Person“

Personenbezogene Daten besonderer Kategorien (Art. 9, 10)

- Daten, aus denen hervorgehen:
  - rassische und ethnische Herkunft,
  - politische Meinungen,
  - religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit,
- genetische und biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
- Gesundheitsdaten oder
- Daten zum Sexualleben oder der sexuellen Orientierung
- Daten über strafrechtliche Verurteilungen und Straftaten

Datenverarbeitung

10 Schritte zum datenschutzkonformen Handeln

Schritt 1: Datenschutzbeauftragter

- prüfen Sie, ob Sie verpflichtet sind, einen Datenschutzbeauftragten zu bestellen
- für den Fall, dass die Verpflichtung besteht,
  - Benennung
  - Veröffentlichung Kontaktdaten
  - Meldung Kontaktdaten an Aufsichtsbehörde

Wann muss ein DSB benannt werden?

für nichtöffentliche Stellen:

- wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen oder
- wenn die Kerntätigkeit in Verarbeitung von Daten besonderer Kategorien besteht → siehe Art. 9
- nach § 38 BDSG (n.F.)
  - **wenn in der Regel mindestens 10 Personen ständig mit der automatisierten DV beschäftigt sind**
  - im Falle von Verarbeitungen, die eine Folgenabschätzung nach Art. 35 DSGVO erfordern → Verarbeitungen mit hohem Risiko für Betroffene
    - Profiling, automatisierte Entscheidungsfindungen
    - umfangreiche Verarbeitung von Daten besonderer Kategorien
    - systematische oder umfangreiche Überwachung öffentlicher Bereiche
  - im Falle geschäftsmäßigen Verarbeitung zum Zwecke der Übermittlung (Adressdatenbanken) oder zum Zwecke der Markt- und Meinungsforschung

Vereins- und Stiftungszentrum
www.vereine-stiftungen.de

Welche Aufgaben hat ein DSB?

- Unterrichtung und Beratung des Verantwortlichen / Auftragsverarbeiters und deren Beschäftigten hinsichtlich ihrer Pflichten nach den einschlägigen Datenschutzvorschriften
- Überwachung der Einhaltung der Datenschutzvorschriften
- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung
- Zusammenarbeit und Anlaufstelle mit/für die Aufsichtsbehörde

Vereins- und Stiftungszentrum
www.vereine-stiftungen.de

Wer kann als DSB benannt werden?

- Mitarbeiter (nicht der Inhaber oder ein Organ des Unternehmens)
- Externe natürliche Person

➢ Voraussetzung: Fachwissen auf dem Gebiet des Datenschutzes, Fähigkeit zur Erfüllung der Aufgaben

Vereins- und Stiftungszentrum
www.vereine-stiftungen.de

Schritt 2: Bestandsaufnahme

- Prüfung
  - Welche Datenverarbeitungstätigkeiten finden im Verein statt?
  - Welche Kategorien von Personen sind hierbei jeweils betroffen?
  - Welche Daten der Betroffenen werden jeweils verarbeitet?
- Dokumentation der Bestandsaufnahme

Dokumentation Bestand

Verarbeitungstätigkeit (Bsp.)	Betroffene	Daten
Kunden- /Klientenverwaltung	Kunden / Klienten	Namen, Adressen, Kontakt-daten, Geburtsdaten, Vertragsdaten, Bankdaten
Interessentenverwaltung	potentielle Kunden	…
Personalverwaltung und -abrechnung	Mitarbeiter	…
Bewerbermanagement	Bewerber,	…
Mitgliederverwaltung	Vereinsmitglieder	…
Beschaffung / Einkauf	Dienstleister, Kunden	…
Betrieb Webseite	Nutzer	IP-Adresse, Dauer, Zeitpunkt, Produkte
Newsletterversand	Adressaten	Name, Mailadresse

Vereins- und Stiftungszentrum
www.vereine-stiftungen.de

Schritt 3: Festlegung der Verarbeitungszwecke

- bestimmen und dokumentieren Sie für jede Verarbeitungstätigkeit den Zweck
- prüfen Sie , ob der Zweck legitim ist
- prüfen Sie, ob alle Daten, die Sie verarbeiten, für den Zweck erforderlich sind
- Löschen Sie Daten, die für den Zweck der Verarbeitung nicht erforderlich sind
- Passen Sie ggf. den Prozess der Datenerhebung an (Bereinigung von Formularen)

Vereins- und Stiftungszentrum
www.vereine-stiftungen.de

Dokumentation Zweckbindung

Verarbeitungstätigkeit	Betroffene	Daten	Zweck
Kunden- /Klientenverwaltung	Kunden / Klienten	…	Vertragsabwicklung
Interessentenverwaltung	potentielle Kunden	…	Kundenakquise
Personalverwaltung und -abrechnung	Mitarbeiter	…	Lohnabrechnung, Abführung Sozialab-gaben/Steuern, Direktion, Arbeitsaufgaben
Bewerbermanagement	Bewerber,	…	Mitarbeiterakquise
Mitgliederverwaltung	Vereinsmit-glieder	…	Verwaltung der Vereinstätigkeit
Beschaffung / Einkauf	Dienstleiste, Kunden	…	Vertragsabwicklung
Betrieb Webseite	Nutzer	…	Außendarstellung
Newsletterversand	Adressaten	…	Mitgliederinfo und Außendarstellung

Vereins- und Stiftungszentrum
www.vereine-stiftungen.de

Schritt 4: Prüfung der Rechtmäßigkeit

Prüfen und dokumentieren Sie, dass die Daten rechtmäßig verarbeitet werden!

- kommen Sie zum Ergebnis, dass Sie Daten ohne entsprechende Rechtsgrundlage verarbeiten, sind diese zu löschen

➢ **Verarbeiten Sie Daten im Auftrag (z.B. eines öffentlichen Leistungsträgers), muss dieser die erforderliche Rechtsgrundlage nachweisen**

Rechtsgrundlagen

Rechtsgrundlagen nach Art. 6 Abs. 1:

a. betroffene Person hat eine qualifizierte Einwilligung erteilt (freiwillig und entsprechend dem definierten Zweck)
b. die 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;
c. die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
d. die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
e. die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
f. die 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, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt

Vereins- und Stiftungszentrum
www.vereine-stiftungen.de

Rechtsgrundlagen bei Daten besonderer Kategorien

Rechtsgrundlagen nach Art. 9 Abs. 2

a. betroffene Person hat eine qualifizierte Einwilligung erteilt (freiwillig und entsprechend dem definierten Zweck)
b. damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann
c. Schutz lebenswichtiger Interessen des Betroffenen oder einer anderen natürlichen Person und der Betroffene kann die Einwilligung aus rechtlichen oder körperlichen Gründen nicht erteilen
d. Verarbeitung durch besondere Organisationen ohne Gewinnerzielungsabsicht im Rahmen ihrer Aufgaben (z.B. Kirche, Gewerkschaften)
e. der Betroffene hat die Daten öffentlich bekannt gemacht
f. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit
g. besondere Rechtsvorschrift des Mitgliedstaates, welches den Wesensgehalt des Rechts auf Datenschutz garantiert → z.B. Sozialdatenschutz
h. Gesundheitsvorsorge und Beurteilung der Arbeitsfähigkeit, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich (soweit gesetzlich geregelt)
i. aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten (soweit gesetzlich geregelt)
j. für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke (soweit gesetzlich geregelt)

Vereins- und Stiftungszentrum
www.vereine-stiftungen.de

Einwilligung

- kommt als Rechtsgrundlage nur die Einwilligung in Betracht, prüfen Sie, ob diese wirksam erteilt wurde und ob sie hierüber entsprechende Nachweise führen können
  - die Wirksamkeit eine mündlich oder konkludent erteilten Einwilligung lässt sich nicht nachweisen!
- eine nach BDSG (alt) rechtmäßig erteilte Einwilligung bleibt wirksam (Düsseldorfer Kreis)
  - Voraussetzung: Freiwilligkeit, schriftlich oder elektronisch mit Widerrufsbelehrung, auf konkreten Verarbeitungsvorgang /Zweck bezogen

Vereins- und Stiftungszentrum
www.vereine-stiftungen.de

Einwilligung

Voraussetzung Wirksamkeit nach DSGVO → Art. 7

- genaue Bestimmung der Zwecke der Datenverarbeitung
- das Ersuchen um Einwilligung muss in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen
- von den anderen Sachverhalten unterscheidbar (kein Verstecken in langen Texten)
- Belehrung über Widerrufsrecht
- Freiwilligkeit → liegt in der Regel nicht vor, wenn die Erbringung einer Leistung davon abhängig gemacht wird, dass der Betroffene seine Einwilligung zur Verarbeitung von solchen Daten erteilt, die für die Erfüllung des Vertrages nicht erforderlich sind

Einwilligung Minderjähriger

- Einwilligung Sorgeberechtigter bei Minderjährigen erforderlich? → Art. 8
  - grundsätzlich nicht, wenn das Kind über die erforderliche Einsichtsfähigkeit verfügt!
  - aber erforderlich bei Kindern U 16 und Angebote von Diensten der Informationsgesellschaft

➢ **Dienste der Informationsgesellschaft**: in der Regel gegen Entgelt im Fernabsatz angebotene und elektronisch abrufbare Dienstleistungen / Waren → BGH (I ZR 117/16): Entgeltlichkeit liegt auch dann vor, wenn das Entgelt nicht vom Nutzer sondern einem Dritten durch Werbemöglichkeiten bezahlt wird (z.B. Soziale Netzwerke, Messengerdienste)

Dokumentation

Dokumentieren Sie das Ergebnis!

Verarbeitungs-tätigkeit	**Betrof-fene**	**Daten**	**Zweck**	**Rechtsgrundlage**
Kunden- / Klientenver-waltung	Kunden	…	…	Durchführung Vertragsverhältnis → Art. 6 Abs. 1 b)
Mitarbeiter-verwaltung	Mit-arbeiter	…	…	Art. 6 Abs. 1 b), Art. 9 Abs. 2 b); Art. 6 Abs. 2 i.V.m. § 26 Abs. 1 und 3 BDSG neu → spezielle Rechtsgrundlage für Arbeitsverhältnisse

Schritt 5: Löschungskonzept

Stellen Sie sicher, dass Daten nicht länger als notwendig gespeichert werden

- prüfen und dokumentieren Sie für jede Verarbeitungstätigkeit, welche Daten Sie wie lange benötigen
  - Kriterien: z.B. Vertragsdauer, Gewährleistungsrechte, Verjährungsfristen, handels-, steuerrechtliche und andere gesetzliche Aufbewahrungsfristen
- prüfen und dokumentieren Sie, in welchen Akten, Programmen und auf welcher Hardware Daten verarbeitet werden
- implementieren Sie einen Prozess, mit welchen Sie sicherstellen, dass Daten nach dem festgelegten Zeitablauf bzw. nach der berechtigten Geltendmachung des Anspruchs auf Löschung oder Einschränkung durch den Betroffenen (gem. Art. 17) auf allen Datenträgern bzw. in allen Datensystemen gelöscht bzw. deren Verarbeitung eingeschränkt werden
- verschieben in Papierkorb genügt nicht!

Schritt 6:
Erfüllung der Informationspflichten

Stellen Sie sicher und dokumentieren Sie, dass Sie Ihre Informationspflichten gegenüber den Betroffenen erfüllen

- Überarbeitung/Erstellung der Datenschutzerklärungen
- Implementierung in die jeweiligen Prozesse (Webseite, Kundenakquise, Arbeitsverträge, Bewerbungsverfahren, Auskunftsverlangen)
- Dokumentation

Vereins- und Stiftungszentrum
www.vereine-stiftungen.de

Welche Informationspflichten bestehen?

- bei Erhebung der Daten gegenüber dem Betroffenen
- wenn Weiterverarbeitung zu anderen Zwecken, als bei Erhebung
- auf Antrag des Betroffenen
- gegenüber Empfängern von Daten, jede Berichtigung, Löschung oder Einschränkung, sofern zumutbar

Vereins- und Stiftungszentrum
www.vereine-stiftungen.de

Wie muss bei Erhebung informiert werden?

bei Erhebung beim Betroffenen	bei Erhebung aus anderen Quellen
• Name und Kontaktdaten des Verantwortlichen, ggf. seines Vertreters	
• ggf. Kontaktdaten des DSB (nicht Name)	
• Zwecke und Rechtsgrundlage, für den Fall dass die Rechtsgrundlage Art. 6 Abs. 1 f) ist, Benennung des berechtigten Interesses die vom Verantwortlichen oder einem Dritten verfolgt werden	
• Empfänger oder Kategorien von Empfängern	
• Ggf. die Absicht der Übermittlung in ein Drittland oder eine intern. Organisation und einen hierfür bestehenden Angemessenheitsbeschluss der EU bzw. bestehende Garantien (EU-US Privacy Shield)	
• Dauer der Speicherung oder die Kriterien für die Festlegung der Dauer	
• Bestehen eines Rechts auf Auskunft, Berichtigung, Löschung Einschränkung, Widerspruch, Datenübertragung	
• Recht auf Widerruf der Einwilligung, wenn das Recht zur Verarbeitung auf einer Einwilligung beruht	
• Recht auf Beschwerde bei Aufsichtsbehörde	
• ggf. Bestehen einer automatisierten Entscheidungsfindung bzw. Profiling und deren Logik und Tragweite	
• ob die Bereitstellung von Daten gesetzl. oder vertragl. vorgeschrieben oder für einen Vertragsschluss erforderlich ist und welche Folgen die Nichtbereitstellung hätte	• Kategorien der Daten, die verarbeitet werden • aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen

Vereins- und Stiftungszentrum
www.vereine-stiftungen.de

Informationen gemäß Art. 13 Datenschutz-Grundverordnung (DS-GVO)
Sehr geehrte Antragsteller,
mit Ihrem Aufnahmeantrag erheben wir von Ihnen personenbezogene Daten. Wir sind gemäß Art. 12 ff. Datenschutzgrundverordnung (DS-GVO) verpflichtet, Ihnen alle Informationen, die sich auf die Verarbeitung dieser Daten beziehen, zu übermitteln. Dieser Verpflichtung kommen wir hiermit nach:

Identität des Verantwortlichen:
Musterverein e.V, Musterstr. 1, 11111 Musterhausen (Tel. xxx, E-Mail: info@muster.de)

Kontaktdaten des Datenschutzbeauftragten: *(nur soweit ein solcher bestellt ist)*
Sie erreichen den zuständigen Datenschutzbeauftragten unter: Datenschutzbeauftragter des Musterverein e.V., Musterstr. 1, 11111 Musterhausen oder datenschutz@muster.de.

Verarbeitungszwecke und Rechtsgrundlage:
Die Datenverarbeitung erfolgt zum Zweck der Mitgliederverwaltung. Hierzu verarbeiten wir Namen, Geburtsdaten, Kontaktdaten, Bankdaten, Daten zur Mitgliedschaft (z.B. Ein- und Austritt, Teilnahme an Veranstaltungen und Versammlungen und Zahlungsinformationen). Weiterer von uns verfolgter Zweck ist die Information der Öffentlichkeit über unsere Tätigkeiten in der Vereinszeitschrift, in Newslettern und auf unserer Webseite sowie die Information von Fördermittelgebern zum Zwecke der Erlangung von Fördermitteln. Für diesen Zweck verarbeiten wir ggf. Namensdaten.
Die Verarbeitung Ihrer Daten zum Zwecke der Mitgliederverwaltung ist nach Art. 6 Abs. 1 Buchstabe b DS-GVO für die Erfüllung Ihrer Mitgliedschaftsrechte und -pflichten erforderlich. Darüber hinaus ist die Datenverarbeitung nach Art. 6 Abs. 1 Buchstabe f DS-GVO zur Wahrung unserer berechtigten Interessen oder der eines Dritten erforderlich. Unsere berechtigten Interessen bestehen in der Erfüllung unseres Vereinszwecks durch öffentliche Wahrnehmung unseres Vereins, den Besuch von Veranstaltungen unseres Vereins durch Dritte sowie der Finanzierung des Vereins durch Besucher, Sponsoren und Fördermittelgeber.

Empfänger:
Zum Zwecke der Information der Öffentlichkeit und von Fördermittelgebern und werden wir, soweit dies erforderlich ist, Namen an Medienunternehmen und Fördermittelgeber übermitteln. Darüber hinaus erfolgt erforderlichenfalls eine Offenlegung bzw. Übermittlung ihrer Daten an unsere externen Dienstleister (z.B. IT-Unternehmen, Buchhaltungsbüros, Steuerberater und Rechtsanwälte) Behörden und Gerichte.

Dauer der Speicherung:
Nach Ende der Mitgliedschaft und Erfüllung aller sich hieraus ergebenden Verbindlichkeiten prüfen wir nach Ablauf von drei Jahren, ob wir Ihre Daten noch benötigen und einer Löschung gesetzliche Aufbewahrungspflichten entgegenstehen. Sofern dies nicht der Fall ist, werden die Daten löschen.

Ihre Rechte:
Ihnen stehen bei Vorliegen der gesetzlichen Voraussetzungen folgende Rechte nach Art. 15 bis 22 DS-GVO zu: Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, auf Datenübertragbarkeit.
Außerdem steht Ihnen nach Art. 14 Abs. 2 Buchstabe c in Verbindung mit Art. 21 DS-GVO ein Widerspruchsrecht gegen die Verarbeitung zu, die auf Art. 6 Abs. 1 Buchstabe f DS-GVO beruht.

Beschwerderecht bei der Aufsichtsbehörde:
Sie haben gemäß Art. 77 DS-GVO das Recht, sich bei der Aufsichtsbehörde zu beschweren, wenn Sie der Ansicht sind, dass die Verarbeitung Ihrer personenbezogenen Daten nicht rechtmäßig erfolgt. Die Anschrift der für unser Verein zuständigen Aufsichtsbehörde lautet: …. *(bitte einfügen)*

Pflicht zur Bereitstellung der Daten:
Die Bereitstellung der Daten ist für den Erwerb der Mitgliedschaft zwingend erforderlich. Sie sind nicht verpflichtet, die Daten bereitzustellen, jedoch kann ohne Bereitstellung der Daten eine Aufnahme in den Musterverein e.V. nicht erfolgen.

Wann muss informiert werden?

- bei Erhebung von Daten beim Betroffenen zum Zeitpunkt der Erhebung
- bei Erhebung von Daten aus andern Quellen bei Kommunikation mit dem Betroffenen oder vor Offenlegung gegenüber Dritten, spätestens einen Monat nach Erlangung
- vor (rechtmäßiger) Weiterverarbeitung zu anderen Zwecken, als bei Erhebung
- auf Antrag des Betroffenen unverzüglich, spätestens innerhalb eines Monats, bei komplexen Fällen Verlängerung um weitere 2 Monate möglich

Dokumentation

Verarbeitungs-tätigkeit	**…**	**Rechtsgrundlage**	**Umsetzung Informationspflicht**
Kunden- / Klientenverwaltung	…	Art. 6 Abs. 1 b)	bei Erhebung Datenschutzerklärung als Anlage zum Vertrag, bei Bestandskunden nachträgliche Übersendung mit Nachweis
Mitarbeiter-verwaltung	…	Art. 6 Abs. 1 b), Art. 9 Abs. 2 b); Art. 6 Abs. 2 i.Vm. § 26 Abs. 1 und 3 BDSG neu → spezielle Rechtsgrundlage Arbeitsverhältnisse	bei Erhebung Datenschutzerklärung als Anlage zum Personalerfassungsbogen , bei Bestandsverträgen nachträgliche Übergabe mit Empfangsbekenntnis
Webseitennutzung, Nutzung Kontaktformular	…	Art 6 Abs. 1 f), Art 6 Abs. 1 a)	bei Erhebung Datenschutzerklärung auf Webseite,

Schritt 7:
Festlegung und Dokumentation technischer und organisatorische Maßnahmen

- Stellen Sie durch angemessene technische und organisatorische Maßnahmen sicher, dass die Rechte und Freiheiten der Betroffenen geschützt sind und dokumentieren Sie die Maßnahmen.
  - Welche Risiken bestehen?
  - Was sind die Riskoquellen?
  - Mit welchen (angemessenen) Maßnahmen kann das Risikopotential gesenkt werden?
- Empfehlung Bayrisches Landesamt für Datenschutz für kleine Vereine: Standardmaßnahmen (aktuelle Betriebssysteme und Anwendungen, Passwortschutz, regelmäßige Backups, Virenscanner, Benutzerrechte)
- Checkliste TOM´s siehe auch:
  www.bdsg-externer-datenschutzbeauftragter.de
  Bei mehreren Verarbeitungstätigkeiten ist Aufteilung in Allgemeinen Teil und Besonderen Teil (separat für jede Verarbeitungstätigkeit zu empfehlen

Schritt 8: Auftragsverarbeitung

Prüfen Sie, ob Sie Daten von Dritten verarbeiten lassen oder selbst Daten im Auftrag verarbeiten und schließen Sie ggf. Verträge mit den erforderlichen Festlegungen!

- Fälle der Auftragsdatenverarbeitung
  - externe Buchhaltung / Lohn- und Gehaltsabrechnung (nicht in Steuerberatungskanzlei s.u.)
  - Softwareentwicklung und –wartung, sofern hierbei Kenntnisnahme personenbezogener Daten
  - Systemmigrationen
  - Externe Wartung von Servern und Computern
  - Webseitenhosting, E-Mail-Hosting
  - Cloud-Computing
  - Mailing (z.B. rapidmail)
  - Datenträgerentsorgung (z.B. Reisswolf)
  - Marketingaktionen durch externe Agentur

Welche Festlegungen muss ein AVV beinhalten?

- Gegenstand, Dauer, Art und Zweck der Verarbeitung
- Art der Daten
- Kategorien der betroffenen Personen
- Pflichten und Rechte des Verantwortlichen (AG)

Festzulegende Pflichten und Rechte des Verantwortlichen (AG)

- Verarbeitung nur auf dokumentierte Weisung des AG
- Verarbeitung nur durch zur Vertraulichkeit verpflichtete Personen
- Sicherstellung, dass der AN entsprechend dem Risiko und der Schwere möglicher Rechtsverletzungen angemessene technische und organisatorische Schutzmaßnahmen ergreift
- Sicherstellung, das Subunternehmer nur nach schriftlicher Genehmigung des AG und Nachweis der für den AN geltenden Pflichten eingesetzt werden
- Sicherstellung, dass der AG alle Rechte des Betroffenen und seine sonstigen Informationspflichten im Falle von Datenschutzpannen gewährleisten kann
- Sicherstellung, dass der AN nach Vertragsbeendigung alle Daten löscht bzw. an den Verantwortlichen zurückgibt (sofern er nicht selbst kraft Gesetzes zur Aufbewahrung verpflichtet ist)
- Kontroll- bzw. Überprüfungsrechte des AG

Vereins- und Stiftungszentrum
www.vereine-stiftungen.de

Schritt 9: Verarbeitungsverzeichnis

Prüfen Sie, ob Sie ein Verfahrensverzeichnis führen müssen und fertigen Sie dieses ggf. an!

- ist schriftlich bzw. elektronisch zu führen
- gilt grds. für den Verantwortlichen und den Auftragsverarbeiter
- gilt nach Art. 30 Abs. 5 DSGVO nicht für Unternehmen, die weniger als 250 Mitarbeiter beschäftigen, es sei denn
  - hohes Risiko für Freiheiten und Rechte der Betroffenen oder
  - **die Verarbeitung erfolgt nicht nur gelegentlich** oder
  - es werden Daten besonderer Kategorien verarbeitet

Vereins- und Stiftungszentrum
www.vereine-stiftungen.de

Inhalt des Verzeichnisses (beim Verantwortlichen)

- Namen und Kontaktdaten des Verantwortlichen und seines DSB
- Alle Verarbeitungstätigkeiten mit den jeweiligen Angaben über
  - Zwecke der Verarbeitung
  - Kategorien der betroffenen Personen und Daten
  - ggf. Kategorien der Empfänger
  - ggf. Drittlandübermittlung und welche geeigneter Garantien für den Datenschutz dort bestehen
  - wenn möglich, die vorgesehen Fristen der Löschung der verschiedenen Datenkategorien
  - Beschreibung der technischen und organisatorischen Maßnahmen

Vereins- und Stiftungszentrum
www.vereine-stiftungen.de

Schritt 10:
Unterrichtung und Verpflichtung Mitarbeiter

- Erstellung einer Datenschutzanweisung (DSA) für Mitarbeiter
- Vermittlung des Inhalts der DSA durch Schulung der Mitarbeiter + Dokumentation
- Verpflichtung der Mitarbeiter auf die Einhaltung der Vertraulichkeit (früher Verpflichtung auf das Datengeheimnis nach § 5 BDSG (alt))
  - Mustervorlage:
    https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_11.pdf

Inhalt einer Datenschutzanweisung

- Information über Begrifflichkeiten
- Information über Pflichten, die Sie als Verantwortlicher oder Auftragsverarbeiter einhalten müssen und die Rechte von Betroffenen
- Festlegung konkreter Verhaltensregeln (entsprechend TOM´s)
- Belehrung über Konsequenzen von Datenschutzverstößen

Konkrete Verhaltensregeln

Beispiele

- Sicherung Zugang Geschäftsstelle Büroräume
  - Verschluss von Fenstern und Türen bei Abwesenheit
  - Empfang / Begleitung von Besuchern im Haus
  - Meldepflichten Schlüsselverlust
- Benutzung Datenverarbeitungssysteme
  - Platzierung Bildschirm bei Publikumsverkehr
  - Passwortschutz
  - Einstellung passwortgeschützter Bildschirmschoner
  - kein Einsatz privater Hardware
  - Umgang mit Druck-, Fax-, Kopiergeräten
  - Umgang mit mobilen Geräten außer Haus (Diebstahlsschutz, Verschlüsselung etc.)
  - Speicherung von Daten auf zentralen Datenträgern (Server), nicht auf Festplatte etc.

Konkrete Verhaltensregeln

- Vorgaben bei Verarbeitung
  - Umgang mit Messengerdiensten,
  - Keine Auskunft ohne sicher Identifikation (z.B. bei Telefonanfragen)
  - Versand von E-Mails mit sensiblen Daten nur verschlüsselt
  - geschützte Aufbewahrung Papierakten
  - Musterschreiben ohne Daten abspeichern
  - sichere Entsorgung Datenträger / Papierakten
- Festlegung von Zuständigkeiten und Verfahren bei
  - Löschungen/Datenberichtigungen/Einschränkungen
  - der Wahrnehmung von Rechten durch einen Betroffenen
  - Verhaltensweisen bei Datenpannen

Vielen Dank für Ihre Aufmerksamkeit!

Vereins- und Stiftungszentrum e.V.
Hertha-Lindner-Str. 10, 01067 Dresden
Tel.: 0351 20 67 00 0
Fax: 0351 20 67 00 19
E-Mail: mail@vereine-stiftungen.de
www.vereine-stiftungen.de

Vereins- und Stiftungszentrum
www.vereine-stiftungen.de