DATEN SCHUTZ AGENTUR

Organisation Technik Compliance

20.06.2018

Leistungsvorschlag Externer Datenschutzbeauftragter

Mit 25.05.2018 wurden aufgrund der neuen Datenschutz-Grundverordnung (DSGVO) neue umfangreiche Datenschutzbestimmungen wirksam. Darüber hinaus traten mit diesem Datum das österreichische Datenschutz-Anpassungsgesetz 2018 und zahlreiche weitere gesetzliche Änderungen in Kraft, die nationale Gesetze an die neuen EU-Datenschutzbestimmungen anpassen. Auf europäischer Ebene wird weiters über eine zusätzliche Datenschutzverordnung für den Bereich der elektronischen Kommunikation (Newsletter, Webseiten, etc) verhandelt. Diese Änderungen sind mit sehr hohen Sanktionsdrohungen verbunden.

Zahlreiche soziale Organisationen stehen daher aktuell vor der Herausforderung, sich rasch an die neuen Bestimmungen des Datenschutzrechts anzupassen und einen rechtskonformen Zustand sicherzustellen. Erschwerend kommt dabei hinzu, dass häufig auch besondere Kategorien von Daten (z.B. Gesundheitsdaten) verarbeitet werden, die ein besonders hohes Schutzniveau erfordern. Die jeweiligen Rahmenbedingungen der Organisationen (Tätigkeitsbereiche, anwendbare Gesetze, Förderverträge, etc) weisen dabei starke Ähnlichkeiten auf.

Vor diesem Hintergrund erscheint es sowohl wirtschaftlich als auch strategisch sinnvoll, gemeinsam einheitliche Vorgangsweisen zu etablieren und Synergieeffekte zu nutzen. Dies kann durch die Bestellung eines externen Datenschutzbeauftragten erreicht werden, der das erforderliche Fachwissen einbringt und organisationsübergreifend auf die Etablierung einheitlicher Datenschutz-Vorgangsweisen hinwirken kann. Diese Standardisierung kann auch gegenüber externen Stellen (Fördergeber, etc) argumentativ gut genutzt werden.

In den folgenden Abschnitten sind die gesetzlichen Aufgaben eines Datenschutzbeauftragten und eine Übersicht möglicher Leistungen wiedergegeben. Für die Übernahme dieser Tätigkeiten schlagen wir folgende Konditionen vor:

- Mindestteilnehmeranzahl: 30 Organisationen
- Monatspauschale: 450 EUR pro Organisation
- Standorte-Beitrag: 20 / 10 EUR pro Monat je Hauptstandort / Nebenstandort
- Stundenumfang / Reisekosten: unbeschränkte Stundenzahl (fair use) / Reisekosten inkludiert
- Dauer der Bestellung: 24 Monate, anschließend Verlängerung jeweils um 12 Monate

mksult GmbH
Kirchberggasse 7/8, 1070 Wien
E: office@datenschutzagentur.com

T: +43 1 480 50 25
F: +43 1 480 50 25 99
www.datenschutzagentur.com

Handelsgericht Wien
UID: ATU63184707
FN 288579g

Hauptstandorte sind Standorte mit medizinischen Einrichtungen, Beratungsstellen, Verwaltungsbüros, Wohnhäusern (betreutes Wohnen), etc, die jährlich im Rahmen von Vor-Ort-Kontrollen auf Einhaltung der Datenschutzvorschriften überprüft werden müssen.

Nebenstandorte sind Standorte mit kleinteiligen Betreuungsangeboten wie z.B. kleine betreute Wohngemeinschaften, die lediglich stichprobenartig im Rahmen von Vor-Ort-Kontrollen auf Einhaltung der Datenschutzvorschriften überprüft werden müssen.

Einvernehmliche Festlegung der Standorte-Anzahl: Die Anzahl der zu berücksichtigenden Haupt- und Nebenstandorte wird im Einzelfall einvernehmlich festgelegt. Maßgeblich ist dafür eine Festlegung, auf welche Weise der verpflichtenden Kontrolltätigkeit des Datenschutzbeauftragten nachgekommen werden kann. Bei einer größeren Anzahl von Standorten bzw. mehreren Standorten mit sehr ähnlichen Tätigkeiten und Abläufen kann ggf. ein Teil der Prüftätigkeit durch die jeweilige Organisation selbst übernommen werden. Im Rahmen der Beitrittsvereinbarung wird in solchen Fällen die Anzahl der durch den Datenschutzbeauftragten zu prüfenden Standorte festgelegt. Nur für diese wird ein Standorte-Beitrag verrechnet. Für die übrigen Standorte prüft der Datenschutzbeauftragte lediglich die Dokumentation der durch die Organisation selbst durchgeführten Prüfungen.

Unbeschränkte Stundenanzahl (fair use): Das vorgeschlagene Modell beruht wesentlich auf der Nutzung von Synergien und Skaleneffekten. Dabei profitieren die einzelnen teilnehmenden Organisationen in großem Umfang von der gemeinsamen Vorgangsweise und der gemeinsamen Nutzung erforderlicher Ressourcen. In diesem Sinne ist bei der Umsetzung darauf zu achten, dass die teilnehmenden Organisationen gleichermaßen von dieser Vorgangsweise profitieren und keine Ungleichgewichte entstehen.

Reisekosten zu allen Standorten innerhalb Österreichs sind inkludiert. Nach Möglichkeit werden auch bei der Reiseorganisation Synergieeffekte bestmöglich genutzt. Allfällig erforderliche Übernachtungskosten werden nach tatsächlichem Aufwand verrechnet.

Abweichende Konditionen für „Hilfsbetriebe“, die z.B. lediglich administrative Aufgaben wahrnehmen, sind möglich und können im Einzelfall einvernehmlich festgelegt werden.

Gesetzliche Aufgaben des Datenschutzbeauftragten

Dem Datenschutzbeauftragten kommt gemäß den Bestimmungen der DSGVO eine beratende und überprüfende Rolle zu. Er berät den für die Verarbeitung Verantwortlichen und die Beschäftigten hinsichtlich ihrer datenschutzrechtlichen Pflichten und überwacht die Einhaltung der Datenschutzbestimmungen sowie der diesbezüglichen Strategien des Verantwortlichen (z.B. die

Zuweisung von Aufgaben, Schulungsmaßnahmen, Überprüfungen, etc.). Die Verantwortung für die Einhaltung sämtlicher datenschutzrechtlicher Bestimmungen verbleibt beim Verantwortlichen. Der Datenschutzbeauftragte haftet als Sachverständiger gemäß den Bestimmungen des § 1299 ABGB.

Im Rahmen der Erstellung von Datenschutz-Folgenabschätzungen wird der Datenschutzbeauftragte in beratender Funktion beigezogen. Der Datenschutzbeauftragte fungiert als Anlaufstelle für die Datenschutzbehörde und arbeitet gegebenenfalls mit dieser zusammen.

Darüber hinaus steht er Betroffenen (das sind sowohl Mitarbeiter als auch Externe) als Ansprechpartner in Datenschutzfragen zur Verfügung. Dabei und im Rahmen der Ausübung seiner übrigen Tätigkeiten ist der Datenschutzbeauftragte an die Wahrung der Geheimhaltung gebunden.

Neben diesen rechtlich vorgesehenen Aufgaben kann der Datenschutzbeauftragte mit weiteren Aufgaben (wie beispielsweise die Führung von Verfahrensverzeichnissen) betraut werden, sofern diese nicht zu einem Interessenskonflikt führen.

Hinsichtlich der organisatorischen Eingliederung sieht die DSGVO vor, dass der Datenschutzbeauftragte frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird und direkten Zugang zur obersten Managementebene erhält.

Leistungsübersicht

Im Rahmen der Tätigkeit als externer Datenschutzbeauftragter können folgende Tätigkeiten übernommen werden:

Erfüllung von Dokumentationspflichten

Führung des Verzeichnisses der Verarbeitungstätigkeiten (Verfahrensverzeichnis)

- Beratung und Unterstützung bei der Bestandsaufnahme der Verarbeitungstätigkeiten
- Durchführung von Abweichungsanalysen gegenüber dem Soll-Zustand nach DSGVO
- Beratung und Unterstützung bei der Erstellung eines priorisierten Maßnahmenplans
- Maßnahmenverfolgung und Überprüfung der rechtskonformen Umsetzung

Erfüllung von Nachweispflichten

- Beratung und Unterstützung bei der Dokumentation der Verarbeitungstätigkeiten zum Nachweis der Einhaltung der Grundsätze der Verarbeitung

- Beratung und Unterstützung bei der Dokumentation von Einwilligungen, Geheimhaltungserklärungen und anderen relevanten Sachverhalten

Dokumentationssystem

- Aufbau und Bereitstellung eines geeigneten Dokumentationssystems

Sicherstellung einer rechtskonformen Verarbeitung

Rechtsgrundlagen der Verarbeitung

- Beratung und Unterstützung bei der Ermittlung von Rechtsgrundlagen der Verarbeitung, der Übermittlung und der Speicherung
- Beratung und Unterstützung bei der Erfüllung von Informationspflichten
- Beratung und Unterstützung bei der Erfüllung von Betroffenenrechten (Auskunft, Berichtigung, Einschränkung, Löschung, etc)
- Beratung und Unterstützung zum rechtskonformen Einsatz von Auftragsverarbeitern (z.B. IT-Dienstleistern)

Risikobewertung

- Beratung und Unterstützung bei der Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen
- Beratung und Unterstützung bei der Auswahl geeigneter technischer und organisatorischer Maßnahmen zur Behandlung dieser Risiken

Datenschutzorganisation

Interne Abläufe und Strategien

- Beratung bei der Planung und Konzeptionierung von Datenschutzstrategien
- Beratung bei der Festlegung interner Vorgaben und Abläufe zur Sicherstellung eines datenschutzkonformen Betriebs (Struktur der Datenschutzorganisation, Richtlinien, Workflows, Zuständigkeiten, etc)
- Beratung bei der Vorbereitung auf die Erfüllung von Betroffenenrechten (Workflows, Kommunikationsstrukturen, Zeitvorgaben, etc)
- Beratung bei der Vorbereitung von Notfallmaßnahmen für Datenschutzverletzungen (Workflows, mögliche Sofortmaßnahmen, Erfüllung von Meldepflichten, etc)

Internes Kontrollsystem

- Beratung bei der Konzeption und Implementierung eines wirksamen internen Kontrollsystems zur Überwachung der Einhaltung der datenschutzrechtlichen Vorgaben

Musterdokumente

- Ausarbeitung und Bereitstellung von Musterdokumenten für die Erfüllung von Betroffenenrechten (Auskunft, Berichtigung, Einschränkung, Löschung, etc)
- Ausarbeitung und Bereitstellung von Musterdokumenten für die Erfüllung von Informationspflichten
- Ausarbeitung und Bereitstellung von Musterdokumenten für Einwilligungen, Geheimhaltungsverpflichtungen, Auftragsverarbeitungen, Datenschutzerklärungen, etc.
- Beratung und Unterstützung bei der Anpassung dieser Musterdokumente für die eigene Organisation

Kontaktstelle

- Datenschutz-Ansprechpartner für
    - Führungskräfte
    - Mitarbeiter
    - Betroffene
    - Datenschutzbehörde
    - Fördergeber, Kontrollstellen und andere externe Partner

Monitoring Datenschutzrecht

- Laufende Überwachung von Änderungen datenschutzrechtlicher Vorschriften
- Laufendes Monitoring der Entscheidungspraxis der Datenschutzbehörde und datenschutzbezogener Gerichtsentscheidungen
- Laufendes Monitoring relevanter Handlungsempfehlungen und Vorgaben des Europäischen Datenschutzausschusses

Kontrolle und Dokumentation

- Beratung beim Aufbau eines internen Datenschutz-Kontrollsystems

- Aufbau und Bereitstellung eines geeigneten Dokumentationssystems (sh. oben bei „Erfüllung von Dokumentationspflichten“)
- Durchführung von Vor-Ort-Kontrollen
- Aufbau und Bereitstellung eines geeigneten Systems zur Maßnahmenverfolgung (Erfassung und Umsetzungskontrolle erforderlicher Optimierungsmaßnahmen)

Berichtswesen

- Laufende Dokumentation datenschutzrelevanter Vorgänge
- Erstellung und Vorlage von Berichten über durchgeführte Vor-Ort-Kontrollen
- Erstellung und Vorlage eines jährlichen Tätigkeitsberichts

Schulungsmaßnahmen

Managementschulungen

- Ausarbeitung und Durchführung von Kompaktschulungen für Führungskräfte

Mitarbeiterschulungen

- Ausarbeitung und Bereitstellung von Schulungsmaterialien für allgemeine Mitarbeiterschulungen (Online-Schulungen)
- Ausarbeitung und Durchführung von Schulungen für die Datenschutz-Ansprechpartner der teilnehmenden Organisationen (Präsenzschulung 1 – 2 Mal jährlich)
- Konzeption von Schulungen zu Spezialthemen (Präsenzschulungen)

Informationsbereitstellung

- Information über aktuelle Themen des Datenschutzes via Newsletter oder Informationsportal

Datenschutz-Folgenabschätzung

Methodik und Durchführung

- Beratung und Unterstützung bei der Auswahl geeigneter Kriterien und Vorgehensweisen zur Erstellung von Datenschutz-Folgenabschätzungen
- Beratung bei der Identifikation von Risiken für die Rechte und Freiheiten betroffener Personen
- Beratung bei der Identifikation geeigneter Maßnahmen zur Behandlung dieser Risiken

- Beratung bei der praktischen Durchführung von Datenschutz-Folgenabschätzungen

Technischer Datenschutz

Datenschutz durch Technikgestaltung

- Beratung bei der Umsetzung der Pflicht zu Datenschutz durch (Technik-)Gestaltung und zu datenschutzfreundlichen Grundeinstellungen

Technisch-organisatorische Maßnahmen (TOMs)

- Beratung bei der Auswahl geeigneter technisch-organisatorischer Maßnahmen zur Sicherstellung eines angemessenen Datenschutzniveaus

Über die Datenschutzagentur

Das auf Datenschutz spezialisierte Beratungsunternehmen mit Sitz in Wien berät Unternehmen, Behörden und andere Organisationen bei der korrekten organisatorischen und technischen Umsetzung der rechtlichen Vorgaben, bei Aufbau und Weiterentwicklung der internen Datenschutzorganisation sowie mit der gutachterlichen Überprüfung der Datenschutzkonformität.

Die Datenschutzagentur ist seit 15 Jahren in der Datenschutzberatung tätig und verfügt über umfangreiche Erfahrungen sowohl mit nationalen und internationalen Unternehmen und Konzernen als auch den relevanten europäischen und nationalen Institutionen und (Datenschutz-)Behörden.

Neben seinem umfangreichen Know-how im Bereich des österreichischen und europäischen Datenschutzes vereint das Team der Datenschutzagentur die Fachbereiche Wirtschaftsinformatik und Recht. Bei der Beratung bringt die Datenschutzagentur ihre Erfahrungen aus der Tätigkeit als Datenschutzbeauftragter im Konzernumfeld, aus der Auditierung von IT-Systemen und der datenschutzrechtlichen und datenschutztechnischen Begutachtung von IT-Produkten und IT-Services in Kundenprojekte ein.

Die Datenschutzagentur begleitet Unternehmen und Organisationen unterschiedlichster Branchen bei der DSGVO-Umstellung und der Durchführung von Datenschutz-Folgenabschätzungen. So zum Beispiel aus den Bereichen der öffentlichen Infrastruktur, der Energiewirtschaft, der Film- und Musikwirtschaft, des Einzelhandels und der Sozialwirtschaft.

Mag. Andreas Krisch ist geschäftsführender Gesellschafter der Datenschutzagentur und seit 2002 im Datenschutz tätig. Er ist Wirtschaftsinformatiker, ausgebildeter betrieblicher und behördlicher Datenschutzbeauftragter sowie technischer und juristischer Gutachter für das Europäische Datenschutz Gütesiegel. Darüber hinaus bringt er umfangreiche Erfahrungen aus den Bereichen Softwareentwicklung und Softwareprojektmanagement in die Beratungsprojekte ein.

Seine Expertise stellte A. Krisch wiederholt europäischen und internationalen Institutionen zur Verfügung und hat unter anderem maßgeblich zur höchstgerichtlichen Abschaffung der verdachtsunabhängigen Vorratsdatenspeicherung in Österreich und der EU beigetragen. Als Mitglied des Datenschutzrates beriet er in den Jahren 2013 bis 2017 die österreichische Bundesregierung.

A. Krisch ist Co-Autor des im MANZ-Verlag erschienen Werkes zur Datenschutz-Grundverordnung sowie Co-Herausgeber und -Autor des Werks Beschäftigtendatenschutz - Handbuch für die betriebliche Praxis.

Für Ihre Datenschutzprojekte steht Ihnen darüber hinaus unser interdisziplinäres Team zur Verfügung, das neben der Spezialisierungsmaterie Datenschutz umfangreiches Know-how aus den Bereichen Wirtschaftsinformatik und Recht in die Beratungsprojekte einbringt.

Referenzen

Die Datenschutzagentur berät laufend nationale wie internationale Unternehmen und Organisationen im Bereich des Datenschutzes und insbesondere der technisch-organisatorischen Umsetzung der rechtlichen Datenschutzanforderungen.

Sie hält dabei auch regelmäßig Kontakt zu den einschlägigen nationalen, europäischen und internationalen Institutionen und hat wiederholt in Expertengruppen der Europäischen Kommission zur Ausgestaltung entsprechender Normen beigetragen.

Wir weisen umfassende Erfahrung im Bereich der Datenschutzberatung vor und besitzen das notwendige Know-how, Ihre Datenverarbeitungsprozesse „fit für die DSGVO“ zu machen. Wir begleiten laufend Unternehmen und andere Organisationen bei der Vorbereitung auf die mit der DSGVO eintretenden Anforderungen und betreuen sie in sämtlichen datenschutzrechtlich relevanten Bereichen.

Aus unseren jüngsten einschlägigen Referenzen erlauben wir uns folgende vorzustellen:

- Die Datenschutzagentur berät laufend **einen der größten österreichischen**

Infrastrukturkonzerne in Datenschutzangelegenheiten. Im Rahmen der Vorbereitung auf die DSGVO führte die Datenschutzagentur die Datenschutz-Folgenabschätzung für eine sehr komplexe Datenverarbeitung des Konzerns durch (mehrere Millionen Betroffene). Weitere Tätigkeiten umfassen unter anderem die Erstellung von Verfahrensverzeichnissen und eines konzernweiten Datenlöschkonzepts.

- Die Datenschutzagentur berät **eine aus rund 80 Gesellschaften bestehende Unternehmensgruppe der Immobilienwirtschaft, der Hotellerie und des Einzelhandels** bei der konzernweiten, mehrere europäische Länder umfassenden Vorbereitung auf die DSGVO.

- Die Datenschutzagentur erstellt für den **führenden Hersteller von Videoanalyse und Videoleitstellenlösungen** regelmäßig datenschutzrechtliche und datenschutztechnische Gutachten über die Funktionalitäten und datenschutzfreundlichen Funktionsweisen seiner IT-Produkte. Im Zentrum steht dabei die Überprüfung der datenschutzfreundlichen Technikgestaltung (Privacy by Design) im Sinne der strengen Kriterien des Europäischen Datenschutz-Gütesiegels EuroPriSe.

- Die Datenschutzagentur berät ein **führendes Unternehmen der internationalen Musik- und Filmwirtschaft** mit Kunden auf allen Kontinenten im Rahmen der Vorbereitung auf die DSGVO. Dabei ist die Datenschutzagentur in allen Projektphasen von der Erfassung des Status Quo bis zur Umsetzung der erforderlichen technisch-organisatorischen Maßnahmen beratend tätig.

- Die Datenschutzagentur berät eine **Vielzahl österreichischer sozialökonomischer Betriebe** in Sachen Datenschutz. In diesem Zusammenhang ist die Datenschutzagentur unter anderem mit folgenden Tätigkeiten betraut: Bestandsaufnahme der bestehenden Datenverarbeitungen; Analyse des Datenaustausches mit Auftraggebern, Fördergebern, staatlichen Einrichtungen und Behörden; Überprüfung des Umgangs mit sensiblen Klientendaten; Schulung von Mitarbeitern; Ausarbeitung von Datenschutz-Handbüchern; Beratung beim Aufbau der betrieblichen Datenschutzorganisation.

- Im Auftrag eines **österreichischen Bundesministeriums** auditierte die Datenschutzagentur die spezifikations- und rechtskonforme Implementierung einer umfangreichen

Individualsoftware. Der Umfang der Tätigkeiten reichte dabei von der Ausarbeitung eines maßgeschneiderten Kriterienkatalogs über die Überprüfung der korrekten Einhaltung fachlicher und datenschutzrechtlicher Anforderungen bis hin zur Ausarbeitung konkreter Maßnahmenvorschläge zur weiterführenden Optimierung.