WIRTSCHAFTSKAMMER ÖSTERREICH

Wiedner Hauptstraße 63 | Postfach 195
1045 Wien
T +43 (0)5 90 900-DW | F +43 (0)5 90 900-243
E rp@wko.at
W http://news.wko.at/rp

Datenschutzbehörde
Wickenburggasse 8
1080 Wien

E-Mail: dsb@dsb.gv.at

Ihr Zeichen, Ihre Nachricht vom	Unser Zeichen, Sachbearbeiter	Durchwahl	Datum
DSB-D056.141/0002-DSB/2019	Rp 1763/19/Ro/MH	3215	12.04.2019

Entwurf einer Verordnung der Datenschutzbehörde, über die Anforderungen an eine Stelle für die Überwachung der Einhaltung von Verhaltensregeln (Überwachungsstellenakkreditierungs-Verordnung - ÜStAkk-V); Stellungnahme

Sehr geehrte Damen und Herren!

Die Wirtschaftskammer Österreich teilt zu dem im Betreff genannten Entwurf Folgendes mit:

Allgemeine Bemerkungen

Bei Unternehmen besteht nach wie vor Rechtsunsicherheit zu vielen Detailfragen der DSGVO, teilweise sogar zu ganz grundsätzlichen Fragen, wie nach der datenschutzrechtlichen Qualifikation als Verantwortlicher oder Auftragsverarbeiter. Aufgrund der weiteren Rechtsfolgen, die an derartig fundamentale Fragen geknüpft sind, ist dies sowohl für Unternehmen als auch für Betroffene ein untragbarer Zustand. Verhaltensregeln (im Folgenden auch „CoC") gem Art 40 DSGVO hätten das Potential, genau diese Rechtsunsicherheit einzudämmen. Im vorliegenden Vorschlag sehen wir allerdings insbesondere Probleme in folgenden drei Bereichen:

1. die unverhältnismäßigen Anforderungen an die Überwachungsstelle,
2. der mit diesen Anforderungen verbundene Finanzierungsbedarf,
3. die Überwachungsverpflichtungen der Überwachungsstellen.

Die Anwendung von CoC gem Art 40 ist für Unternehmen jeweils optional und wird naturgemäß nur erfolgen, wenn diese einem Unternehmen mehr Vor- als Nachteile bringen. Aus der Sicht eines Unternehmens ist davon auszugehen, dass die Nachteile der genannten Kernprobleme in ihrer derzeitigen Form viel schwerer wiegen, als der Vorteil einer allfälligen Rechtssicherheit. Durch Bescheid bestätigte CoC einer Branche bieten eine gewisse Form der Rechtssicherheit, dies unabhängig davon, ob sich ein konkretes Unternehmen diesen Regeln selbst unterwirft oder nicht. Anzunehmen ist, dass die Datenschutzbehörde zwei gleiche Sachverhalte/Verarbeitungstätigkeiten von unterschiedlichen Unternehmen nicht allein deshalb rechtlich unterschiedlich bewerten wird, nur weil sich ein Unternehmen den CoC unterworfen hat und das andere nicht. CoC präzisieren die DSGVO nur und ändern diese nicht.

Obgleich die Benennung einer Überwachungsstelle nach Artikel 41 Abs 1 DSGVO nicht ausdrücklich zwingend vorgesehen ist („... **kann** die Überwachung der Einhaltung von

Verhaltensregeln gemäß Artikel 40 von einer Stelle durchgeführt werden, die über das geeignete Fachwissen hinsichtlich des Gegenstands der Verhaltensregeln verfügt und die von der zuständigen Aufsichtsbehörde zu diesem Zweck akkreditiert wurde"), wird im Rahmen der Abstimmung unter den Datenschutzbehörden im EDSA von einer diesbezüglichen Verpflichtung ausgegangen. Weder Artikel 40 Abs 4 DSGVO noch Artikel 41 Abs 1 DSGVO schreiben jedoch eindeutig die obligatorische Benennung einer solchen Stelle vor. Vielmehr verweist Artikel 40 Abs 4 DSGVO lediglich darauf, dass CoC iSd Artikel 40 Verfahren vorsehen müssen, welche einer in Artikel 41 Absatz 1 genannten Stelle ermöglichen, die obligatorische Überwachung auszuüben, nicht jedoch, dass die Überwachungsstelle selbst obligatorisch zu bestellen wäre. Auch die bisherigen CoC nach § 6 Abs 4 DSG 2000 schrieben eine derartige Stelle nicht vor, zumal eine Schlichtungs- oder Überwachungsstelle zweifelsfrei freiwillig bestellt werden konnte.

Gemäß Art 40 Abs 1 DSGVO haben Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission die Ausarbeitung von CoC eigentlich zu fördern. Die gesetzten Anforderungen an die vermeintlich obligatorisch zu bestellende Überwachungsstelle würden allerdings die Ausarbeitung von CoC wesentlich erschweren, wenn nicht sogar verhindern. Diesbezüglich muss auch die Finanzierung einer solchen Stellen bedacht werden.

Wir befürchten daher in der jetzigen Form sogar Nachteile für Unternehmen, wenn sich diese CoC unterwerfen. Eine Überwachungsstelle ist nun in irgendeiner Form zu finanzieren, was nach der jetzigen Einschätzung wohl durch die Überwachten selbst zu erfolgen hat; gleichzeitig müssten sich diese zusätzlichen Überwachungsmaßnahmen (zB Überprüfungsverfahren) aussetzen. Dieser Umstand führt dazu, dass kaum ein Unternehmen die CoC annehmen wird. Das verhindert wiederum die Finanzierung (und fachkundliche Besetzung) der Überwachungsstelle.

Zu den einzelnen Bestimmungen des Entwurfs

Zu § 2:
Hinsichtlich der Akkreditierung von Überwachungsstellen iSd Art 41 DSGVO scheinen die Leitlinien des EDSA durchaus flexibler gestaltet zu sein als es der Entwurf der ÜStAkk-V vorgibt. Insbesondere sollte auch hier die Möglichkeit der externen sowie internen Bestellung der Überwachungsstelle unterstützt werden, da dies einige Optionen auch für die einreichenden Verbände offenlassen würde. Naturgemäß muss eine gewisse organisatorische Trennung vorgenommen werden, um die unabhängige Einhaltung zu gewährleisten, insbesondere sollte eine Weisungsunabhängigkeit dargestellt werden. Dies würde auch dem Bild des Datenschutzbeauftragten nach Art 37ff DSGVO entsprechen. Auch der betriebliche Datenschutzbeauftragte kann Mitarbeiter des Unternehmens sein, darf nur nicht dem Leitungsgremium angehören und es darf kein Interessenkonflikt entstehen. Ein ähnliches Prozedere und ähnliche Voraussetzungen sollten auch für die Überwachungsstelle und deren Mitarbeiter gelten.

Nach den Erläuterungen zu § 2 Abs 1 ist es sowohl für juristische als auch für natürliche Personen möglich, als Überwachungsstelle akkreditiert zu werden. Demnach wäre es auch möglich und legitim, eine Einzelperson, welche die übrigen Voraussetzungen nach der ÜStAKK-V erfüllt, als Überwachungsstelle namhaft zu machen bzw zu akkreditieren. Das ist durchaus zu begrüßen, bringt dieser Punkt doch wesentliche Erleichterungen für die Wirtschaft.

Dies spricht wohl auch (entgegen der Bemerkung in Kapitel 12.8 der Leitlinien (Guidelines) zu Verhaltensregeln und diesbezüglichen Überwachungsstellen des EDSA) für ein informelles Gremium, bestehend aus verschiedenen Personen / Stakeholdern / Experten,

was eine enorme Hilfestellung für die einreichenden Verbände mit sich bringen würde, da externe Vereinsgründungen oÄ die Erstellung von CoC erschweren.

Wir regen hier zB an, die Möglichkeit als Überwachungsstelle zu fungieren, auch nicht ins Firmenbuch bzw Vereinsregister eingetragenen Unternehmen bzw Gremien zu ermöglichen. Insbesondere Arbeitskreisen sollte die Möglichkeit eröffnet werden, als Überwachungsstelle agieren zu können.

Gerade in kleineren Branchen, die sich Verhaltensregeln freiwillig unterwerfen, wird es vermutlich wenige Beschwerdefälle geben. Hier sollte vor allem in Anbetracht unserer Vorbemerkung ein niederschwelliger Zugang zur Etablierung einer Überwachungsstelle gewählt werden, da ansonsten der Zugang zu Verhaltensregeln in eher kleineren Branchen massiv gefährdet wird.

Als formale Anmerkung erlauben wir uns darauf hinzuweisen, dass in § 2 Abs 2 Z 1 lit a mehrere Verweise auf andere Rechtsmaterien inkl Angaben von BGBl gemacht werden. Beim Verweis auf das Vereinsgesetz 2002 wird die BGBl-Zahl unvollständig wiedergegeben. Hier wird lediglich die BGBl-Zahl, aber nicht die Jahreszahl angeführt. Korrekterweise müsste es lauten: „(...) VerG, BGBl I Nr. 66/2002 (...)". Vgl ebenso BGBl Nr. 194 bezüglich der Gewerbeordnung 1994.

Die „nach außen Vertretungsbefugten" gem § 2 Abs 2 Z 1 lit b sollten in den Erläuterungen konkretisiert werden.

In Übereinstimmung mit den Erläuterungen zu § 2 Abs 2 Z 1 lit c (Seite 2) könnte zur Klarstellung folgende Formulierung im Verordnungstext zu § 2 Abs 2 Z 1 lit c gewählt werden: „c) *bei natürlichen Personen* allenfalls die Berufsbezeichnung ..."

§ 2 Abs 2 Z 3 weist aus, das angestrebte Fachgebiet müsse durch Bezugnahme und Definition auf die Verbände und andere Vereinigungen deklariert werden. Nach den Erläuterungen hierzu ist auch die Benennung mehrerer Fachgebiete möglich. (Dies sollte sich aus dem Verordnungstext selbst ergeben: *„3. das angestrebte Fachgebiet bzw die angestrebten Fachgebiete ...")*.
Aus dieser Formulierung könnte herausgelesen werden, dass - ähnlich dem bisherigen Modell der Zertifizierungsstellen - eine Akkreditierung auch unabhängig von konkreten CoC nach Artikel 40 DSGVO angesucht werden kann. Dies erschiene tatsächlich wirtschaftlich sinnvoll, da zum einen eine gewisse Konkurrenz an Anbietern gegeben wäre, was eine regelmäßige Evaluierung der Tätigkeit der Überwachungsstelle ermöglichen würde, zum anderen wären die Finanzierungskonzepte wohl durchaus realistischer. Man denke hier weiters auch an allenfalls notwendige Wechsel von Überwachungsstellen. Müssten die Ersteller von CoC nach Artikel 40 DSGVO erst bei Ausfall einer bisherigen Überwachungsstelle eine neue Stelle akkreditieren lassen, würde dies einige zeitliche Verzögerung und damit Unsicherheit für jene Verantwortliche und Auftragsverarbeiter mit sich bringen, welche sich den CoC unterworfen haben. Der (allenfalls mitunter vertragsrechtlich notwendige) Wechsel einer Überwachungsstelle wurde bislang weder von Seiten des EDSA noch von Seiten der österreichischen Datenschutzbehörde thematisiert.

Die Bestimmung des § 2 Abs 4 scheint missverständlich: Es sollte bei der Pflicht zur Übersetzung nicht auf einen inländischen Antragsteller, sondern darauf abgestellt werden, in welcher Sprache die „Dokumente und Urkunden" verfasst sind.

Der Entwurf verwendet in §§ 2 Abs 3 und 4, 3 Abs 1, 4 Abs 3 und 6 Abs 1 die Wendung „Dokumente und Urkunden". Es sollte zumindest in den Erläuterungen eine Klarstellung erfolgen, was unter dem jeweiligen Begriff zu verstehen ist bzw worin sich diese Begriffe

unterscheiden. Andernfalls könnten sich unnötige Unsicherheiten bspw bei der Beurteilung der Beweiskraft ergeben.

Auch ist grundsätzlich die Tatsache zu hinterfragen, dass - entgegen dem Grundsatz der Unbeschränktheit der Beweismittel nach § 46 AVG - der Entwurf lediglich „Dokumente und Urkunden" als Nachweis vorsieht. Wiewohl die Akkreditierungsverfahren wohl tendenziell „urkundenlastig" ausgestaltet sein werden, scheint eine Einschränkung im Verordnungswege nicht geboten. Art 41 DSGVO fordert, dass Unabhängigkeit, Fachwissen etc leidglich „zur Zufriedenheit ... der Aufsichtsbehörde nachgewiesen" werden müssen.

Zu § 3:
Weder im Verordnungstext noch in den Erläuterungen hierzu ist ersichtlich, wer die Voraussetzungen für eine Überwachungsstelle gemäß § 3 zu erfüllen hat und was diese konkret sind. Beispielsweise stellt sich bei der Besetzung in Gremien die Frage, ob die Voraussetzungen von einer Person in der Überwachungsstelle erfüllt werden müssten oder von allen Personen. Es macht aus unserer Sicht keinen Sinn, die Voraussetzungen an bestimmte Personen zu knüpfen, da dies zur Folge hätte, dass bei einem Wechsel der Personen in der Überwachungsstelle, diese erneut akkreditiert werden müsste (die Problematik in diesem Fall wurde bereits zu § 2 ausgeführt). Da letztendlich das Gremium und nicht einzelne Personen akkreditiert werden würden, wenn ein Gremium als Überwachungsstelle genannt wird, sollten die Voraussetzungen auch nur insgesamt im Gremium betrachtet erfüllt werden.

Nach § 3 Abs 2 darf die Überwachungsstelle in keinem rechtlichen, wirtschaftlichen, persönlichen oder fachlichen Abhängigkeits- bzw Naheverhältnis zu den zu Überwachenden stehen, wobei eine Finanzierung der Überwachungsstelle der Unabhängigkeit grundsätzlich nicht entgegensteht, soweit die Kosten von allen zu Überwachenden zu entrichten sind (vgl Erläuterungen zu § 3 Abs 2). Wie sieht dies iF einer Finanzierung der Überwachungsstelle durch die Ersteller der CoC aus? Oftmals ist in CoC kein zusätzlicher Kostenbeitrag der Überwachenden vorgesehen, sondern eine entsprechende Finanzierungsregelung durch jene Verbände oder Vereinigungen, welche die CoC formuliert haben. Jene Verbände bzw Vereinigungen werden üblicherweise durch Mitgliedsbeiträge ihrer Mitglieder finanziert. Müssten nun CoC eine für die Überwachenden kostenpflichtige Lösung integrieren, andernfalls die Objektivität und Unabhängigkeit der Überwachungsstelle in Frage gezogen werden würde? Es muss sichergestellt sein, dass einreichende Verbände (zB auch Verbände, welche die gesetzliche Interessenvertretung als Körperschaften öffentlichen Rechts ausführen) auch als Überwachungsstelle (intern wie extern) fungieren können.

Durch die Offenlegung der wirtschaftlichen Eigentümer in § 3 Abs 3 Z 1 wird es der Datenschutzbehörde ermöglicht zu überprüfen, ob die Überwachungsstelle nicht mit einem zu überwachenden Verantwortlichen oder Auftragsverarbeiter wirtschaftlich verbunden ist oder durch personelle Verflechtungen zwischen Überwachungsstelle und einer zu überwachenden Stelle ein Interessenskonflikt besteht. Als Beispiel hierfür wird ausgeführt, dass der Geschäftsführer der Überwachungsstelle nicht gleichzeitig in einer Führungsposition beim Überwachten tätig ist.

Ist diese Vorschrift auf gesellschaftsrechtliche Führungspositionen beschränkt zu sehen (worauf der Verweis auf die wirtschaftlichen Eigentümer und das Wirtschaftliche Eigentümer Registergesetz, WiEReG, schließen lässt) oder sind hier beispielsweise auch Juristen, Datenschutzbeauftragte oder Techniker in den Unternehmen der Überwachten gemeint? Gerade diese verfügen über das notwendige fachliche Knowhow und die entsprechende Branchenkenntnis. Zwar gelten Datenschutzbeauftragte als unabhängig iSd Artikel 37ff DSGVO, sind jedoch auch beratend und unterstützend tätig, was wiederum in den Erläuterungen zu § 3 Abs 2 als „fachliche Abhängigkeit" gesehen wird. Jedenfalls sollte klargestellt werden, dass die Beratung der zu Überwachenden durch einzelne Mitglieder

eines Kollegialorganes nicht der fachlichen Unabhängigkeit der Überwachungsstelle entgegensteht.

Da für die Überwachungsstelle gewisse Branchenkenntnis und fachliches Knowhow notwendig sind, wäre es - bei einer Beibehaltung des § 3 Abs 2 in der jetzigen Form - schwierig, geeignete Mitglieder für die Überwachungsstelle zu finden, da die Voraussetzungen für den Nachweis an das erforderliche fachliche Wissen überbordend formuliert sind.

Es ist im Hinblick auf § 3 Abs 2 und 3 unbedingt erforderlich, weitere Klarstellungen und/ oder Erleichterungen hinsichtlich der Vorgaben und des Nachweises der Unabhängigkeit der Überwachungsstelle aufzunehmen, widrigenfalls die auf Papier geforderte Unabhängigkeit kaum gewährleistet werden kann, zumal auch ein gewisses Fachwissen verlangt wird, welches naturgemäß nur innerhalb der jeweilig einreichenden Branche zur Verfügung gestellt werden kann. Zu verweisen ist in diesem Zusammenhang auch auf die Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 vom 12. Februar 2019, welche hinsichtlich der Akkreditierungsvoraussetzungen durchaus erleichterte Ansätze verfolgen (beispielsweise wäre auch die Akkreditierung eines „internal monitoring body" unter gewissen Voraussetzungen möglich.)

In diesen vom Europäischen Datenschutzausschuss herausgegebenen Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 sind in Rz 62 ff **externe oder interne** Überwachungsstellen vorgesehen; siehe https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under_de:

„62. The GDPR provides flexibility around the type and structure of a monitoring body to be accredited under Article 41. Code owners may decide to use **external or internal** monitoring bodies provided that in both cases the relevant body meets the accreditation requirements of Article 41 (2) as outlined in the eight requirements listed below.

64. There are **two main models of monitoring which could be used** by code owners for fulfilling the monitoring body requirements: **external and internal monitoring body. There is some flexibility within these two types of monitoring approaches and different versions could be proposed** which are appropriate given the context for the code. Examples of internal monitoring bodies could include an ad hoc internal committee or a separate, independent department within the code owner. It will be for the code owners to explain the risk management approach with regard to its impartiality and independence.

65. For instance, where an internal monitoring body is proposed, there should be separate staff and management, accountability and function from other areas of the organisation. This may be achieved in a number of ways, for example, the use of effective organisational and information barriers and separate reporting management structures for the association and monitoring body. Similar to a data protection officer, the monitoring body should be able to act free from instructions and shall be protected from any sort of sanctions or interference (whether direct or indirect) as a consequence of the fulfilment of its task."

Nach den im Entwurf zur Überwachungsstellenakkreditierungs-VO vorgesehenen Bestimmungen liegt die Unabhängigkeit der Überwachungsstelle (nur) vor, wenn die Überwachungsstelle in keinem derart rechtlichen, wirtschaftlichen, persönlichen oder fachlichen Abhängigkeits- oder Naheverhältnis zu den zu Überwachenden steht, das ihr Urteil und ihre Unabhängigkeit und Integrität bei ihrer Tätigkeit als Überwachungsstelle in Frage stellen könnte. Damit könnte gemeint sein, dass nur externe Überwachungsstellen ausreichend unabhängig iSd Verordnung sind. Dies würde ein Gold Plating zu den Bestimmungen in Art 41 DSGVO darstellen.

Es sollte daher jedenfalls klargestellt werden, dass auch interne Überwachungsstellen akkreditiert werden können.

Betont wird auch nochmals, dass die Voraussetzungen für einen Nachweis über ausreichend Fachwissen nach § 3 Abs 4 zu hoch angesetzt sind.

Als einschlägige Ausbildung sollte im Übrigen grundsätzlich auch die Gewerbeberechtigung der Unternehmensberatung gelten, zumal diese Ausbildung nicht nur profunde Kenntnisse über den Aufbau und die Organisationsstruktur von Unternehmen mit sich bringt, sondern auch im Hinblick auf Art 37 ff DSGVO als relevant für die Bestellung eines Datenschutzbeauftragten angesehen wird.

Zu § 4:
Artikel 41 Abs 2 lit b DSGVO weist aus, die Überwachungsstelle müsse Verfahren festlegen, die es ihr ermöglichen zu bewerten, ob Verantwortliche und Auftragsverarbeiter die Verhaltensregeln anwenden können, die Einhaltung der CoC durch die Verantwortlichen und Auftragsverarbeiter überwachen und die Anwendung der CoC regelmäßig zu überprüfen. Ein regelmäßiges Audit, wie in den Erläuterungen zu § 4 ausgewiesen, jedes Unternehmens, das sich den CoC unterwirft, ist kaum zu bewerkstelligen, zumal selbst Zertifizierungen, die gemäß Artikel 42 DSGVO vorgesehen sind, für eine Dauer von drei Jahren erteilt werden könnten.

Ein erhöhtes Maß an administrativem Aufwand (in Form von in zu kurzen Abständen verpflichtend durchzuführenden Audits) wird im Sinne der Verfahrensvereinfachung strikt abgelehnt.

Zudem ist fraglich, was unter „regelmäßig" zu verstehen ist, da beispielsweise die Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 vom 12. Februar 2019 zu 12.4., Rz 72 „annual inspections" thematisieren. Derartige Anforderungen können möglicherweise in vergleichsweise kleinen Branchen mit enormem Aufwand erfüllt werden, Verbände mit bis zu 10.000 Mitgliedsunternehmen oder mehr, welche sich potentiell den CoC anschließen möchten, haben keine derartigen Möglichkeiten.

Am Beispiel der Buchhaltungsberufe zeigt sich transparent, welche Folgen die beschriebenen Überwachungsmaßnahmen hätten. Bei ca 10.000 Berufsberechtigten müsste die Überwachungsstelle 10.000-mal pro Jahr eine „Überwachung der Einhaltung der CoC" durchführen, die (nach Abzug von Wochenenden und Feiertagen) an ca 250 Arbeitstagen vorzunehmen sind. Das sind 40 Überwachungsmaßnahmen pro Tag. Selbst wenn keine jährliche Überprüfung, aber eine regelmäßige vorgesehen wäre (zB regelmäßig in Fünfjahresabständen?), wären es ca 8 Überwachungsmaßnahmen pro Tag. Wie viele Vollzeitstellen müsste eine Überwachungsstelle haben, um dies leisten zu können?

Das Argument, dass sich wohl nicht alle Berufsberechtigten den CoC unterwerfen, ist wohl zutreffend. Trotzdem sollte das System nicht so eingerichtet werden, dass es nur dann funktioniert, wenn sich möglichst wenige daran beteiligen. Es sollte den einreichenden Verbänden überlassen bleiben, wie diese eine entsprechende Überwachungstätigkeit durchführen können und sollte sich diese auch nach den Gegebenheiten des einzelnen CoC und der Anzahl an Mitgliedsunternehmen richten können.

Zu § 5:
§ 5 enthält Vorgaben zum Streitbeilegungsverfahren der Überwachungsstelle. § 5 Abs 3 Z 2 legt hierzu iF kollegialer Entscheidungsgremien „das Recht der Parteien" fest, „eine von ihnen ernannte natürliche Person in das Gremium zu entsenden". Inwiefern dies mit den

vorherigen Bestimmungen in Übereinstimmung gebracht werden kann, ist fraglich. Diese Bestimmung ist zudem unklar, da der Ausdruck „Parteien" nicht näher definiert wird, wohl aber die „Verfahrensparteien" des Streitbeilegungsverfahren gemeint sein könnten, was bedeuten würde, dass ad-hoc Gremien gebildet werden müssten (sofern die Überwachungsstelle als Gemium aufgebaut werden würde), in welche sowohl betroffene Person als auch Überwachende jemanden entsenden könnten / müssten. Das ist aufgrund des enormen bürokratischen Aufwands schlicht abzulehnen, zumal dies keinen Anhaltspunkt in Artikel 40 oder Artikel 41 DSGVO findet. Es muss den Antragstellern zur Akkreditierung der Überwachungsstelle überlassen bleiben, wie ein allfälliges Beschwerdeverfahren abgewickelt werden sollte.

Zu § 6:
In § 6 Abs 1 wird nach den Erläuterungen Art 41 Abs 4 DSGVO umgesetzt. In Art 41 Abs 4 wird jedoch auch vorgesehen, dass Maßnahmen nur „... *vorbehaltlich geeigneter Garantien* ..." zu setzen sind. Darunter wird in der Literatur verstanden, dass die Überwachungsstelle keine Maßnahmen zu setzen braucht, wenn der von einer allfälligen Maßnahme betroffene Verantwortliche oder Auftragsverarbeiter bereits selbst tätig geworden ist, um künftige Verletzungen wirksam zu unterbinden[1]. Eine derartige Möglichkeit sollte auch in der Verordnung explizit vorgesehen werden.

Hinsichtlich § 6 Abs 2 sollte zumindest in den Erläuterungen klargestellt werden, ob es sich um eine taxative Aufzählung handelt.

Nach Abs 3 soll die ergriffene Maßnahme dem Verantwortlichen oder Auftragsverarbeiter schriftlich bekanntzugeben sein.
In den Erläuterungen heißt es, dass Maßnahmen der Überwachungsstelle „ihrem Wesen nach zivilrechtlicher Natur" sind und daher gegen sie auch kein Beschwerderecht an die Datenschutzbehörde zustehe. Streitigkeiten mit der Überwachungsstelle seien daher ausschließlich auf dem Zivilrechtsweg auszutragen. Die Überwachungsstelle habe der Datenschutzbehörde jährlichen einen Tätigkeitsbericht vorzulegen, damit diese ihre Aufsichtspflicht erfüllen könne. Davon unberührt bleibe die Verpflichtung der Überwachungsstelle, die Datenschutzbehörde über die von ihr verhängten Maßnahmen und deren Begründung zu unterrichten.
Die Pflicht zur Begründung ergriffener Maßnahmen wird demnach nur in den Erläuterungen und auch dort nur im Zusammenhang mit der gebotenen Unterrichtung der Datenschutzbehörde erwähnt. Aufgrund der möglichen Auswirkungen von Maßnahmen auf die betroffenen Verantwortlichen und Auftragsverarbeiter erscheint dies jedoch als eine nicht ausreichende Verankerung. Um eine Maßnahme zivilrechtlich einer Überprüfung unterziehen und sich gegen zu Unrecht ergriffene Maßnahmen schützen zu können, sollte die Begründungspflicht im Verordnungstext erwähnt und der Überwachungsstelle diese Pflicht ausdrücklich auch gegenüber dem Verantwortlichen und dem Auftragsverarbeiter auferlegt werden.
§ 6 Abs 3 sollte daher lauten: *„Die ergriffene Maßnahme ist dem Verantwortlichen oder Auftragsverarbeiter schriftlich bekannt zu geben und zu begründen."*

Gemäß § 6 Abs 4 hat die Überwachungsstelle jährlich einen Bericht bis zum 31. März über die im vorangegangenen Jahr erfolgten Tätigkeiten vorzulegen. Eine derartige Berichterstattung an die Datenschutzbehörde ist vor allem deshalb überschießend, weil dies von Artikel 40 oder 41 DSGVO nicht verlangt wird. Art 41 Abs 4 DSGVO sieht zwar eine Unterrichtung über Maßnahmen vor, allerdings ist uE die geplante Berichtspflicht wohl nicht unter diese „Maßnahmenunterrichtung" subsumierbar.

---

[1] Strohmaier in *Knyrim*, DatKomm Art 41 DSGVO Rz 33 (Stand 1.12.2018, rdb.at).

Der in § 6 geforderte jährliche Bericht über die erfolgten Tätigkeiten im vorangegangenen Jahr wird als administrativ zu aufwändig und nicht zielführend abgelehnt.
Zudem wird dies - wie ausgeführt - in Artikel 40 oder 41 DSGVO nicht verlangt. Wir sprechen uns deshalb vehement gegen dieses geplante Gold Plating aus.

Werden Verbände und Vereinigungen, welche Unternehmen vertreten, tatsächlich angehalten, vermehrt CoC iSd Artikel 40 DSGVO für ihre Branchen zu erstellen, um einerseits Unsicherheiten in der Branche klären zu können, andererseits aber wohl auch um die Datenschutzbehörde in „einfacheren Beschwerdefällen" entlasten zu können (zumal der Beschwerdeweg an die DSB selbstverständlich offen steht, wird angenommen, dass eine externe Schlichtung durchaus Zulauf finden und dadurch die Beschwerdeanzahl bei der DSB verringert wird), müssen auch Rahmenbedingungen geschaffen werden um diesen Wunsch erfüllen zu können.

Wenn Verhaltensregeln im Sinne der Rechtssicherheit für Branchen aber auch zur Entlastung der Datenschutzbehörde abgeschlossen werden sollen, so muss den Branchen auch eine praxisnahe, zeitökonomische und administrativ zu bewältigende Umsetzung durch die entsprechenden Rahmenbedingungen zugestanden werden.

Mit freundlichen Grüßen

Dr. Rosemarie Schön
Abteilungsleiterin