Datenschutzbehörde
Wickenburggasse 8 2
1080 Wien

E-Mail: dsb@dsb.gv.at

Wien, am 23.04.2019

BETREFF: ISPA STELLUNGNAHME ZUM ENTWURF DER ÜBERWACHUNGSSTELLEN-AKKREDITIERUNGS-VERORDNUNG

Sehr geehrte Damen und Herren,

die ISPA erlaubt sich im Zusammenhang mit der öffentlichen Konsultation der Datenschutzbehörde zum Entwurf einer Verordnung über die Anforderungen an eine Stelle für die Überwachung der Einhaltung von Verhaltensregeln (Überwachungsstellenakkreditierungs-Verordnung – ÜStAkk-V), wie folgt Stellung zu beziehen.

Zusammengefasst spricht sich die ISPA dafür aus, dass der Verordnungsentwurf die Akkreditierung sowohl von internen als auch von externen Überwachungsstellen zulassen soll. Zudem soll die Zuständigkeit für die Antragstellung für die Akkreditierung einer Aufsichtsstelle im Entwurf näher ausgelegt werden, um die Verordnung anwenderfreundlicher zu gestalten. Im Sinne der Rechtssicherheit und Transparenz betont die ISPA zudem, dass eine eindeutige Verknüpfung der Aufsichtsstelle mit den jeweiligen Verhaltensregeln zwingend erforderlich ist. Im Sinne der Kosteneffizienz und einer ökonomischen Verwaltung sind als Gremien aufgestellte Aufsichtsstellen als eine Einheit zu akkreditieren und nicht deren einzelne Mitglieder. Hinsichtlich der Unabhängigkeitsanforderungen an die Überwachungsstelle in § 3 des Entwurfs soll *Gold Plating* hintangehalten werden, da diese in der Praxis kaum zu gewährleisten sind und zur Hemmung der Erarbeitung von Verhaltensregeln führen würden, wobei die DSGVO diese Prozesse explizit fördern möchte. Zudem merkt die ISPA an, dass die fachlichen Anforderungen an die Überwachungsstelle im Entwurf zu hoch angesetzt sind und fordert, dass eine verpflichtende Überprüfung durch die Überwachungsstelle im Sinne der Ressourceneffizienz nur in Anlass- oder Beschwerdefällen erfolgen soll. Aus Sicht der ISPA sind Berichtspflichten an die DSB überschießend und werden auch nicht von der DSGVO verlangt.

1. **Die Verordnung soll die Akkreditierung sowohl von internen als auch von externen Überwachungsstellen zulassen**

Laut den Erwägungen zu § 2 Abs 1 muss die akkreditierte Stelle nicht an eine bestimmte Rechtsform (z.B. Kapitalgesellschaft oder Personengesellschaft) geknüpft werden. Nach den Erläuterungen zu § 2 Abs 1 ist es sowohl für juristische als auch 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 wesentliche Erleichterungen für die Wirtschaft.

Die Bestimmung könnte jedoch auch sehr restriktiv ausgelegt werden, nämlich, dass eine Aufsichtsstelle jedenfalls eine eigene Rechtspersönlichkeit haben soll und somit nur außerhalb des für die Verhaltensregeln federführenden Verband angesiedelt sein kann. Daher weckt der Entwurf den Eindruck explizit für die Akkreditierung von externen Aufsichtsorganen konzipiert zu sein. Diese Einschränkung widerspricht jedoch den Leitlinien des Europäischen Datenschutzausschusses[1], welche durchaus erleichterte Ansätze verfolgen, indem sie die Akkreditierung sowohl von externen als auch von internen Aufsichtsstellen zur Überwachung der Einhaltung von Verhaltensregeln zulassen.

> "[…] *Code owners may decide to use external or internal monitoring bodies provided that in both cases the relevant body meets the accreditation requirements* […]"[2]

Aus Sicht der ISPA soll eine Überwachungsstelle sowohl intern im Rahmen des federführenden Verbands eines Code of Conduct als auch extern als eigene Rechtspersönlichkeit angesiedelt werden können. Durch die Ermöglichung einer größeren Vielfalt an Lösungen für die Ausgestaltung einer Überwachungsstelle würde auch die Datenschutzbehörde ihren gesetzlichen Auftrag, die Ausarbeitung von Verhaltensregeln zu fördern, nachkommen.

Die ISPA lehnt eine derart restriktive Ausgestaltung des Verordnungsentwurfs ab, und fordert, dass dieser dahingehend neu überdacht wird, dass die Akkreditierung sowohl von internen als auch von externen Aufsichtsstellen, im Sinne der Leitlinien des europäischen Datenschutzausschusses, ermöglicht wird.

2. **Die Zuständigkeit für die Antragstellung für die Akkreditierung einer Aufsichtsstelle soll im Entwurf näher ausgelegt werden**

Ferner ist in § 2 Abs. 2 des ÜStAkk-V Entwurfs festgehalten, dass die Identität des Antragsstellers anhand von verschiedenen Unterlagen und Urkunden nachzuweisen ist. Es ist jedoch aus dem Verordnungsentwurf nicht ableitbar, wer letztlich für die Antragsstellung für die Akkreditierung

[1] EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, version for public consultation, in Internet: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-20190219_guidelines_coc_public_consultation_version_en.pdf (12.04.2019)
[2] EDPB Guidelines, Rz 62, Seite 20, in Internet: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-20190219_guidelines_coc_public_consultation_version_en.pdf (12.04.2019)

eines Überwachungsorgans zuständig ist. Es ist unklar, ob sich diese Bestimmung auf den Verband, welcher die Genehmigung der Verhaltensregeln erwirkt hat, oder auf die Überwachungsstelle an sich, die akkreditiert werden soll, bezieht.

Im konkreten Fall des Code of Conduct für ISPs ist nicht nachvollziehbar, ob der Antrag von der ISPA als federführender Verband oder vom Aufsichtsbeirat gestellt werden soll. Die zweite Option bestärkt erneut den Eindruck, dass die Behörde eine sehr restriktive Position hinsichtlich der Ausgestaltung der Überwachungsstelle vertritt, nämlich, dass diese nur außerhalb des federführenden Verbands angesiedelt werden darf. Diese restriktive Position ist aus Sicht der ISPA strikt abzulehnen.

ISPA vertritt zudem die Meinung, dass sofern es ich um eine interne Aufsichtsstelle handelt, der Antrag jedenfalls vom für die Ausarbeitung der Verhaltensregeln verantwortlichen Verband einzureichen ist. Daher regt die ISPA eine diesbezügliche Klarstellung im Verordnungsentwurf an, die zu mehr Rechtssicherheit und einer anwenderfreundlicheren Ausgestaltung der Verordnung beitragen wird.

3. Im Sinne der Rechtssicherheit und Transparenz ist eine eindeutige Verknüpfung der Aufsichtsstelle mit den jeweiligen Verhaltensregeln zwingend erforderlich

Laut § 2 Abs 2 Z 3 des Entwurfs muss das angestrebte Fachgebiet durch Bezugnahme und Definition auf die Verbände und andere Vereinigungen deklariert werden. Nach den Erläuterungen hierzu ist auch die Benennung mehrerer Fachgebiete möglich. Aus dieser Formulierung könnte herausgelesen werden, dass – ähnlich dem bisherigen Modell der Zertifizierungsstellen – eine Akkreditierung auch unabhängig von konkreten Verhaltensregeln nach Artikel 40 DSGVO angesucht werden kann.

Da der Verordnungsentwurf in seiner derzeitigen Fassung scheinbar keinen Konnex zwischen den Verhaltensregeln und der Aufsichtsstelle herstellt, weck dieser somit den Eindruck, dass auch externe Stellen, welche in keiner Verbindung zu bereits genehmigten Verhaltensregeln stehen, sich einseitig für die Überwachung von Codes of Conduct zuständig erklären können, sofern diese als Aufsichtsorgan für den jeweiligen Fachbereich akkreditiert wurden.

Aufgrund der eingriffsintensiven Maßnahmen, die eine Überwachungsstelle treffen kann, ist es für die Unternehmen, die sich einem Code of Conduct unterwerfen, unabdingbar Klarheit darüber zu haben, wer für die Überwachung der Einhaltung des jeweiligen Code of Conduct zuständig ist. Daher spricht sich die ISPA im Sinne der Transparenz und Rechtssicherheit dafür aus, dass eine Verlinkung der Verhaltensregel mit einer konkreten Aufsichtsstelle zwingend erforderlich ist.

In dem konkreten Fall des ISPA Code of Conduct für ISPs bezieht sich auch der bereits genehmigte Teil des Code of Conduct auf den Aufsichtsbeirat als Überwachungsorgan. Daher wäre aus Sicht der ISPA eine legistische Lösung, welche eine einseitige Zuständigkeitserklärung einer für den Fachbereich Telekom akkreditierten, externen Stelle zulassen würde, strikt

abzulehnen. Daher regt die ISPA an, dass der Verordnungsentwurf in diesem Punkt neu überdacht wird.

4. Im Sinne der Kosteneffizienz und einer ökonomischen Verwaltung sind Aufsichtsgremien als eine Einheit zu akkreditieren

In § 3 des Entwurfs sind die Voraussetzungen für eine Überwachungsstelle aufgezählt. Aus dem Entwurf ist es jedoch schwer zu entnehmen, wer diese Voraussetzungen erfüllen muss. Beispielsweise stellt sich bei der Besetzung in Gremien wie beim ISPA Aufsichtsbeirat die Frage, ob die Voraussetzungen von den einzelnen Mitgliedern zu erfüllen sind oder von der Überwachungsstelle als Ganzes.

Aus Sicht der ISPA ist es nicht zielführend, 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 müssten. Daher spricht sich die ISPA im Sinne der Kosteneffizienz und einer ökonomischen Verwaltung dafür aus, dass im Falle von Gremien die Aufsichtsstelle als eine Einheit akkreditiert werden muss, um bei einem allfälligen Mitgliederwechsel eine neue Akkreditierung des Überwachungsorgans zu vermeiden.

5. Hinsichtlich der Unabhängigkeitsanforderungen an die Überwachungsstelle in § 3 des Entwurfs soll *Gold Plating* hintangehalten werden

Nach § 3 Abs 2 des Entwurfs darf eine Überwachungsstelle in keinem rechtlichen, wirtschaftlichen, persönlichen oder fachlichen Abhängigkeits- bzw. Naheverhältnis zu den zu Überwachenden stehen. Laut den Erläuterungen zu § 3 Abs 2 steht eine Finanzierung des Aufsichtsorgans der Unabhängigkeit grundsätzlich nicht entgegensteht, soweit die Kosten von allen zu Überwachenden zu entrichten ist.

Oftmals ist in Verhaltensregeln kein zusätzlicher Kostenbeitrag der Überwachenden vorgesehen, sondern eine entsprechende Finanzierungsregelung durch jene Verbände oder Vereinigungen, welche die Verhaltensregeln formuliert haben. Jene Verbände bzw. Vereinigungen werden üblicherweise durch Mitgliedsbeiträge ihrer Mitglieder finanziert. Aus Sicht der ISPA ist es nicht erforderlich, dass Verhaltensregeln eine für die Überwachenden kostenpflichtige Lösung integrieren müssen, um die Objektivität und Unabhängigkeit der Überwachungsstelle zu gewährleisten.

Die Unabhängigkeit und Objektivität des Überwachungsorgans kann vielmehr einerseits durch die Aufsichtsstelle selbst sichergestellt werden, indem allfällige Herausforderungen oder Interessenkonflikte proaktiv beispielsweise im Rahmen einer Geschäftsordnung adressiert werden. Diese soll Mechanismen enthalten, welche im Falle eines potenziellen Interessenskonflikts bereits Handlungsoptionen bietet, die die Unabhängigkeit und Unparteilichkeit der Überwachungsstelle gewährleisten. Anderseits könnte die Unabhängigkeit und die Objektivität eines internen

Überwachungsgremiums auch zusätzlich durch den Einsatz effektiver Organisations- und Informationsbarrieren durch den federführenden Verband erreicht werden.

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 Auftragsverantwortlichen wirtschaftlich verbunden ist oder durch personelle Verflechtungen zwischen Überwachungsstelle und einer zu überwachenden Stelle ein Interessenskonflikt besteht. Als Beispiel wird ein Geschäftsführer der akkreditierten Stelle genannt, der gleichzeitig auch bei der zu überwachenden Stelle in einer Führungsposition tätig ist.

Im Lichte des ISPA Aufsichtsbeirats, welcher u.a. aus vier Datenschutzbeauftragten besteht, die in einem zu überwachenden Unternehmen tätig sind, hebt die ISPA hervor, dass Datenschutzbeauftragte grundsätzlich gemäß Art. 37 DSGVO per Gesetz unabhängig sind, dabei kann es sich um einen internen oder externen Datenschutzbeauftragten handeln. Wenn diese besondere Stellung von Datenschutzbeauftragten berücksichtigt wird, und zudem bedacht wird, dass ein interner Datenschutzbeauftragter unabhängig und weisungsfrei handelt, obwohl dieser in dem zu kontrollierenden Unternehmen integriert ist, dann entspricht eine Aufsichtsstelle zweifelsohne den hohen Unabhängigkeitsstandards der DSGVO, da diese nicht in die Organisation des zu überwachenden Unternehmens integriert ist. Diese Personenkategorie stellt sich als besonders geeignet dar, um allfällige beanstandete Verstöße durch die unterzeichnenden Unternehmen untersuchen zu können, da sie die unternehmensinterne Perspektive bei der Umsetzung der datenschutzrechtlichen Anforderungen besonders gut kennen.

In diesem Zusammenhang betont die ISPA erneut, dass die Unabhängigkeit eines Aufsichtsgremiums als Gesamtheit und nicht jene der einzelnen Mitglieder nachzuweisen ist. Daher sollten auch weitere Umstände, die für die Sicherstellung der Unabhängigkeit und der gewissenhaften Ausübung der Pflichten im Rahmen des Aufsichtsorgans relevant sind, wie die Anzahl der Mitglieder oder die von ihnen vertretenen Institutionen, wie sektorspezifische Aufsichtsbehörden oder wissenschaftliche Einrichtungen, berücksichtigt werden, um die Eignung des jeweiligen Gremiums als Aufsichtsstelle beurteilen zu können.

Zusammengefasst sind aus Sicht der ISPA die Unabhängigkeitsanforderungen an die Überwachungsstelle, wie im Entwurf der Datenschutzbehörde vorgesehen, überschießend und stellen ein *Gold Plating* im Vergleich der Vorgaben der DSGVO und der Leitlinien des europäischen Datenschutzausschusses dar. Daher ist im Hinblick auf § 3 Abs 2 und 3 unbedingt erforderlich, dass weitere Klarstellungen und Erleichterungen hinsichtlich der Vorgaben und des Nachweises der Unabhängigkeit des Aufsichtsorgans aufgenommen werden, widrigenfalls ist die im Entwurf geforderte Unabhängigkeit kaum zu gewährleisten, zumal auch ein gewisses Fachwissen verlangt wird, welches naturgemäß nur innerhalb der jeweilig einreichenden Branche zur Verfügung gestellt werden kann. Zudem regt die ISPA an, dass der Verordnungsgeber die Unabhängigkeitsanforderungen an die Leitlinien des europäischen Datenschutzausschusses anpasst und dadurch für mehr Flexibilität bei der Ausgestaltung der Aufsichtsstellen sorgt.

Ferner würden diese aus Sicht der ISPA überschießenden Anforderungen an Überwachungsstellen in der Praxis dazu führen, dass sich kaum geeignete Personen finden werden, um an solchen Aufsichtsstellen teilzunehmen. Dies würde wiederum die Erarbeitung von Verhaltensregeln hemmen, wobei die DSGVO diese Prozesse explizit fördern möchte, um höhere Datenschutzstandards, unter Berücksichtigung der sektorspezifischen Besonderheiten der jeweiligen Branche, zu schaffen. Diesen Bestrebungen des europäischen Gesetzgebers sollte die Datenschutzbehörde entsprechend Rechnung tragen und im Entwurf der ÜStAkk-V widerspiegeln.

6. Die fachlichen Anforderungen an die Überwachungsstelle im Entwurf sind zu hoch angesetzt

In § 3 Abs. 4 des Verordnungsentwurfs sind die fachlichen Anforderungen an eine Überwachungsstelle enthalten, welche u.a. den Abschluss eines einschlägigen Studiums an einer Universität oder einer FH oder fünfjährige einschlägige Tätigkeit in dem Fachgebiet sowie ausgezeichnete Kenntnisse des Datenschutzrechts voraussetzen. Im Detail ist ein einschlägiges Studium, jedenfalls Rechtswissenschaften, Informatik oder der Abschluss einer auf Datenverarbeitung spezialisierten berufsbildenden höheren Schule oder alternativ fünf Jahre einschlägige berufliche Tätigkeit in dem jeweiligen Fachgebiet jedenfalls als ausreichend anzusehen, um Eignung zu belegen. Auch eine Zertifizierung gilt als einschlägige Ausbildung.

Aus Sicht der ISPA sind die Anforderungen für einen Nachweis über ausreichend Fachwissen zu hoch angesetzt. Eine mindestens fünfjährige einschlägige Tätigkeit im jeweiligen Fachgebiet wird beispielsweise von der Vorsitzenden der Datenschutzbehörde selbst verlangt, jedoch nicht von einfachen Mitarbeitern in der Datenschutzbehörde. Derartig hohe Anforderungen können nicht an eine Überwachungsstelle von ohnehin zu genehmigenden Verhaltensregeln nach Art. 40 DSGVO gestellt werden. Als einschlägige Ausbildung sollte 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 Artikel 37 ff DSGVO als relevant für die Bestellung eines Datenschutzbeauftragten angesehen wird.

Daher regt die ISPA an, dass die fachlichen Anforderungen an die Überwachungsstelle neu überdacht und erleichtert werden, um ein *Gold Plating* hintanzuhalten. Auch hier gelten die Bedenken der ISPA, dass die ausufernden Anforderungen an Überwachungsstellen in der Praxis zur Hemmung der Erarbeitung von Verhaltensregeln führen würden. Diese Entwicklung würde eindeutig das Ziel der DSGVO konterkarieren, nämlich Codes of Conduct zu fördern. Daher regt die ISPA an, dass die DSB die Anforderungen an die Überwachungsstellen im Entwurf der ÜStAkk-V entsprechend erleichtert, um die Realisierbarkeit dieser auch in der Praxis zu gewährleisten und dadurch die Erarbeitung von Verhaltensregeln zu fördern.

7. Eine verpflichtende Überprüfung durch die Überwachungsstelle soll im Sinne der Ressourceneffizienz nur in Anlass- oder Beschwerdefällen erfolgen

Gemäß § 4 des Verordnungsentwurfs hat die Überwachungsstelle ein Verfahren festzulegen, um die Einhaltung der Verhaltensregeln zu überwachen und die Anwendung der Verhaltensregeln regelmäßig überprüfen zu können. In den Erläuterungen zu § 4 wird zudem erörtert, dass auch ein Verfahren sowie Strukturen einzurichten sind, die die Einhaltung der Verhaltensregeln aktiv überwachen, wie beispielsweise durch Stichprobenprüfungen und Auditierungen. Sie kann aber auch verpflichtende (periodische) Berichterstattungen der den Verhaltensregeln unterworfenen Unternehmen verlangen.

Ein jährliches Audit, wie in den Erläuterungen zu § 4 ausgewiesen, jedes Unternehmens, das sich den Verhaltensregeln unterwirft, ist sehr aufwendig und kaum zu bewerkstelligen, zumal selbst Zertifizierungen, die gemäß Artikel 42 DSGVO vorgesehen sind, für eine Dauer von drei Jahren erteilt werden könnten. In diesem Fall werden die Überprüfungen auch nicht jährlich vorgenommen. Ferner ist diese Maßnahme auch nicht in der DSGVO vorgesehen.

Darüber hinaus weist die ISPA darauf hin, dass die DSGVO Vereine und Verbände versucht zu motivieren, Verhaltensregeln zu erstellen. Eine gehäufte aktive Überprüfung der Unternehmen würde jedoch sowohl Vereine als auch Unternehmen im Gegenteil davon abschrecken DSGVO Codes of Conduct zu erstellen bzw. sich diesen zu unterwerfen. Dadurch wird auch dem Hauptziel der DSGVO, nämlich ein hohes Datenschutzniveau sicherzustellen, konterkariert.

Aus Sicht der ISPA ist es überschießend, wenn sich ein Unternehmen einer jährlichen Überprüfung unterziehen muss, nur aufgrund seiner Teilnahme an den Verhaltensregeln. Daher regt die ISPA im Sinne der Ressourceneffizienz eine verpflichtende Überprüfung durch die Überwachungsstelle nur in Anlass- oder Beschwerdefällen an. Zusätzlichen zu aktiven Überprüfungen sollten auch Audits von zertifizierten externen Stellen an die Überwachungsstelle vorgelegt werden können.

8. Berichtspflichten an die DSB sind überschießend und werden auch nicht von der DSGVO verlangt

Gemäß § 6 Abs 4 hat die Überwachungsstelle jährlich einen Bericht bis zum 31. März über die im vorangegangenen Jahr erfolgten Tätigkeiten vorzulegen. Aus Sicht der ISPA sind auch die Berichtspflichten an die DSB überschießend und werden auch nicht von der DSGVO verlangt.

Unter dem Gesichtspunkt, dass Verbände und Vereinigungen angehalten werden, vermehrt Verhaltensregeln iSd Artikel 40 DSGVO für ihre Branchen zu erstellen, um einerseits sektorspezifische sowie datenschutzrechtliche Fragestellungen im Rahmen der Umsetzung der DSGVO klären zu können, andererseits aber wohl auch um die Datenschutzbehörde in „einfacheren Beschwerdefällen“ entlasten zu können, ist diese bürokratische Verpflichtung nicht sonderlich zielführend. Um diese entlastende Funktion der Überwachungsstelle auch in der Praxis

gewährleisten zu können und dadurch die Beschwerdeanzahl bei der DSB zu verringern, müssen auch entsprechende Rahmenbedingungen geschaffen werden.

Die ISPA hofft auf die Berücksichtigung ihrer Bedenken und Anregungen.

Für Rückfragen (und weitere Auskünfte) stehen wir jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen,

ISPA - Internet Service Providers Austria

Dr. Maximilian Schubert

Generalsekretär

Die ISPA – Internet Service Providers Austria – ist der Dachverband der österreichischen Internet Service-Anbieter und wurde im Jahr 1997 als eingetragener Verein gegründet. Ziel des Verbandes ist die Förderung des Internets in Österreich und die Unterstützung der Anliegen und Interessen von rund 220 Mitgliedern gegenüber Regierung, Behörden und anderen Institutionen, Verbänden und Gremien. Die ISPA vertritt Mitglieder aus Bereichen wie Access, Content und Services und fördert die Kommunikation der Marktteilnehmerinnen und Marktteilnehmer untereinander.