BUNDESARBEITSKAMMER
PRINZ EUGEN STRASSE 20-22
1040 WIEN
wien.arbeiterkammer.at
DVR 0063673
ERREICHBAR MIT DER LINIE D

Bundesministerium
für Öffentlichen Dienst
und Sport
Hohenstaufengasse 3
1010 Wien

Ihr Zeichen	Unser Zeichen	Bearbeiter/in	Tel **501 65**	Fax **501 65**	Datum
BMöDS-920.196/0002-III/1/2018	SP-GSt	Martina Chlestil	DW 12419	DW 142419	27.2.2018

Datenschutz-Anpassungsgesetz – Dienstrecht

Die Bundesarbeitskammer (BAK) bedankt sich für die Übermittlung des im Betreff genannten Entwurfs und nimmt dazu wie folgt Stellung:

Zweck der Änderungen

Mit dem vorliegenden Entwurf erfolgen Anpassungen in den datenschutzrechtlichen Bestimmungen in den Dienstrechten an die Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG – Datenschutz-Grundverordnung (im Folgenden: DS-GVO).

Zusammenfassende Bewertung

Begrüßt wird das eingangs definierte Ziel, dass mit dem Entwurf erforderliche Anpassungen an die DS-GVO vorgenommen werden und auch eine Beschreibung der wesentlichen Maßnahmen erfolgt. Wichtig ist für die BAK, dass an einem hohen Datenschutzniveau für die Betroffenen (zumeist Bediensteten, StellenbewerberInnen) festgehalten werden muss.

Dazu erlaubt sich die BAK einige Anregungen:

- Werden personenbezogene Daten besonderer Kategorien verarbeitet, sind besondere Datensicherheitsmaßnahmen vorzusehen.

- Die Zielrichtung der statistischen Gewährleistung von Anonymität bei der Einleitung allgemeiner Kontrollmaßnahmen der IKT-Nutzung von Bediensteten durch das Abstellen auf

Organisationseinheiten mit einer Mindestanzahl an Bediensteten, um (vorerst) Rückschlüsse auf einzelne Bedienstete grundsätzlich auszuschließen, ist beizubehalten.

- Eine Stellungnahmemöglichkeit der von Kontrollmaßnahmen betroffenen Bediensteten sowie von zumutbaren Unterstützungsmaßnahmen durch die IT-Stelle ist zu normieren, um Verdachtsmomente vorab aufklären bzw entkräften zu können.

- Protokolldaten über lesende Zugriffe und Protokolldaten über ändernde Zugriffe im Rahmen der Kontrollmaßnahmen der §§ 79e ff BDG sollen so lange aufzubewahren (und dem jeweils betroffenen Bediensteten einsichtig) sein, wie der Datenbestand, auf den zugegriffen wurde, aufbewahrt wird.

- Um der Maxime eines hohen Datenschutzniveaus durchgängig zu entsprechen, sollten die durch Öffnungsklauseln eingeräumten Regelungsspielräume der DS-GVO, insbesondere nach Art 23 DS-GVO, nicht dazu genutzt werden, um Rechte der Betroffenen, wie das Recht auf Berichtigung, Löschung etc zu allgemein und undifferenziert zu beschneiden.

- Umfassende Mitwirkungsrechte der Interessenvertretung bei der Verarbeitung von personenbezogenen Daten sind sicherzustellen, um die Schutzinteressen der Bediensteten zu wahren.

Zu den einzelnen Bestimmungen

Beamten-Dienstrechtsgesetz 1979 (BDG)

§ 79e, § 79f, § 79g neu:

Personenbezogene Daten besonderer Kategorien – Datensicherheitsmaßnahmen

Im derzeit in Geltung stehenden § 79e Abs 2 BDG wird bei der Durchführung von Kontrollmaßnahmen auf die Verwendung von „personenbezogenen Daten“ abgestellt. Werden die Begriffsbestimmungen des bis zum 24.5.2018 noch geltenden DSG 2000 zu Grunde gelegt, dann sind damit im Sinne des § 4 Z 1 DSG 2000 Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist, gemeint. Von diesem übergeordneten Datenbegriff abzugrenzen sind „sensible Daten“, die gemäß § 4 Z 2 Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben sind. Die Verwendung auch von „sensiblen Daten“, die einen erhöhten Schutz genießen müssen, ist vom Wortlaut des BDG nicht ausdrücklich mitumfasst. Der nun vorliegende Entwurf weitet jedoch die Kategorien der Daten, die verarbeitet werden dürfen, ausdrücklich auch auf diese „sensible“ Datenkategorie aus. Ein Grund dafür ist in den Erläuterungen nicht zu finden. Nun sollen zusätzlich zu den nicht-sensiblen personenbezogenen Daten ausdrücklich auch „personenbezogene Daten besonderer Kategorien“, dh terminologisch grundsätzlich die ehedem „sensiblen Daten“, verar-

beitet werden dürfen. Darunter sind im Sinne des Art 9 DS-GVO Daten, aus denen die rassische und ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugung oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung zu verstehen. Auch wenn nachvollzogen werden kann, dass im Zusammenhang mit der Kontrolle der (auch privaten) IKT-Nutzung von Bediensteten unter Umständen durchaus auch besondere Kategorien von Daten (im Rahmen des Verhältnismäßigkeitsgrundsatzes) verarbeitet werden müssen (zB der Aufruf von Webseiten eines Gesundheitsdiensteanbieters), so erscheint es der BAK jedenfalls erforderlich, diese Ausdehnung verarbeitbarer Datenkategorien im gegenständlichen Zusammenhang näher darzulegen.

Die BAK anerkennt, dass die Daten gem § 79e Abs 2 und gem § 79g Abs 1 BDG in der vorgeschlagenen Fassung nur dann verarbeitet werden dürfen, soweit dies für die näher beschriebenen rechtmäßigen Zwecke erforderlich ist und nicht die Interessen oder Grundrechte und Grundfreiheiten einer bzw eines Bediensteten überwiegen.

Dennoch erlaubt sich die BAK auf folgendes hinzuweisen:

Art 9 DS-GVO, der die Verarbeitung „sensibler Daten“ (neue Terminologie: „Besondere Kategorien personenbezogener Daten“) in bestimmten, taxativ aufgelisteten Fällen erlaubt, verlangt in seinen Ausnahmebestimmungen (zum grundsätzlichen Verarbeitungsverbot) grosso modo geeignete und spezifische Schutzmaßnahmen hinsichtlich der Grundrechte und der Datenschutz-Interessen der betroffenen Personen. Mit anderen Worten müssen wegen der Sensibilität dieser Daten Datensicherheitsmaßnahmen in strikterer Form als bei einer Verarbeitung nicht-sensibler Daten ergriffen werden; macht ein Mitgliedstaat von einer diesbezüglichen Öffnungsklausel Gebrauch, müssen diese prozeduralen, technischen und organisatorischen Maßnahmen als generelle Vorkehrungen auch im entsprechenden nationalen Recht vorgesehen werden.

Begutachtungsgegenständlich ist auszuführen, dass die Gebrauchmachung des österreichischen Gesetzgebers (wohl) von der Möglichkeit des Art 9 Abs 2 lit b DS-GVO vermittels der Bestimmungen der §§ 79e ff BDG in Form des Festschreibens des bloßen Dürfens der Verarbeitung auch „personenbezogener Daten besonderer Kategorien“ sohin unionsrechtlich nicht hinreicht; vielmehr ist der Gesetzgeber gemäß Art 9 Abs 2 lit b DS-GVO hierbei zusätzlich verpflichtet, „geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person“ vorzusehen.

Solches ist mit der vorgeschlagenen Fassung der besagten Normen überwiegend nicht geschehen, sodass sich selbst bei Gesetzwerdung Selbiger nichts am diesbezüglichen Verarbeitungsverbot dieser („sensiblen“) Daten ändern würde. Um dem entsprechenden Verarbeitungswillen des Gesetzgebers zum Durchbruch zu verhelfen, wären insbesondere die folgenden Datensicherheitsmaßnahmen, die ua der aktuellen Kommentar-Literatur zur DS-GVO entnommen sind, gesetzlich vorzuschreiben:

- Strenge Zweckbindung samt einem ausdrücklichen Zweckänderungsverbot (nicht nur im Fall des § 79f Abs 5 BDG).

- Stellungnahmerecht (samt einer verpflichtenden Dokumentation einer solchen Stellungnahme) einer/eines betroffenen Bediensteten (zusätzlich zu den Informationsrechten gemäß §§ 79f Abs 2 und 5 sowie 79g Abs 3 und 7 BDG).

- Einbindung der Personalvertretung (in Form eines schriftlichen Informationsrechtes) auch in den Fällen des § 79f BDG (Gefahr eines Schadens für die IKT-Infrastruktur) analog § 9 Abs 3 lit o PVG.

- Verpflichtung zur sofortigen Löschung personenbezogener Daten, sollte sich der Verdacht einer gröblichen Dienstpflichtverletzung nicht bestätigen; Verpflichtung zur sofortigen Löschung personenbezogener Daten, wenn keine weitere Gefährdungslage für die IKT-Infrastruktur oder ihre korrekte Funktionsfähigkeit mehr besteht.

- Verarbeitung dieser besonderen Datenkategorie nur durch besonders (datensicherheits- und datenschutzrechtlich) geschultes und in wiederkehrenden Abständen nachzuschulendes IT-Fachpersonal, das einer besonders strengen Verschwiegenheitspflicht zu unterwerfen ist.

- Zuerkennung eines Berufsgeheimnisschutzes an dieses IT-Fachpersonal.

Die Verarbeitung besonderer Kategorien von personenbezogenen Daten kann nach dem neuen unionalen Datenschutzrecht die Durchführung einer Datenschutz-Folgenabschätzung gemäß Art 35 DS-GVO erforderlich machen. Regelt eine nationale Rechtsvorschrift die konkreten Verarbeitungsvorgänge, kann gemäß Art 35 Abs 10 DS-GVO bereits im Rahmen der allgemeinen Gesetzesfolgenabschätzung eine solche Datenschutz-Folgenabschätzung vorweggenommen werden; das sollte mit dem vorliegenden Gesetzesentwurf gemäß den Erläuterungen der Fall sein. Dies erscheint nach Ansicht der BAK allerdings insofern nicht ausreichend, als dabei nicht zwischen nicht-sensiblen und „sensiblen“ personenbezogenen Daten unterschieden wird (was natürlich dem Umstand geschuldet ist, dass auch der Gesetzgeber für die „sensible“ Datenkategorie gegenständlich keine besonderen Datensicherheitsvorkehrungen vorsieht). Für letztere wären nämlich – wie bereits ausgeführt – verstärkte Datensicherheitsmaßnahmen zu normieren und zu bewerten; insofern bleibt die Frage offen, ob die zuständigen Dienststellen letztlich in bestimmten Einzelfällen von Kontrollmaßnahmen, bei denen auch „sensible“ Daten verarbeitet werden, nicht doch vorab eine Datenschutz-Folgenabschätzung vorzunehmen verpflichtet wären, wenn der Gesetzgeber hier nicht entsprechend „nachbessert“.

Die BAK regt daher an, im BDG (bzw PVG) besondere Datensicherheitsmaßnahmen der geschilderten Art vorzusehen, wenn diese personenbezogenen Daten besonderer Kategorien verarbeitet werden. Zudem wird darauf hingewiesen, dass diese Datensicherheitsmaßnahmen auch laufend zu evaluieren sind. Eine entsprechende Normierung auch dieser (unions-

rechtlich neuen) Datensicherheitsanforderung ist in den Gesetzestext aufzunehmen; die näheren Regelungen können einer Verordnung (insbesondere der IKT-Nutzungsverordnung BGBl II 2009/281) vorbehalten werden.

§ 79e Abs 4 neu:

Ausweitung der Kontrollmaßnahmen

Nach der derzeit geltenden Rechtslage des § 79e Abs 4 BDG dürfen sich Kontrollmaßnahmen nur auf Organisationseinheiten mit mindestens fünf Bediensteten beziehen. Wird diese Anzahl in einer Organisationseinheit nicht erreicht, so ist die jeweils übergeordnete Organisationseinheit miteinzubeziehen. Der vorliegende Entwurf sieht nun den Entfall dieser statistischen Grenze vor und regelt stattdessen, dass sich Kontrollmaßnahmen nur auf die unbedingt erforderliche Anzahl an Bediensteten beziehen dürfen. Die Abänderung der Regelung folgt laut den Erläuterungen aus der Umsetzung des Grundsatzes der Datenminimierung. Diese Zielrichtung, wonach Kontrollmaßnahmen nicht flächendeckend erfolgen, sondern sich nur auf die unbedingt erforderliche Anzahl an Bediensteten beziehen sollen, ist nachvollziehbar und begrüßenswert. Allerdings darf dabei eine weitere Zielrichtung des Datenschutzes und überhaupt des Regelungskonzeptes der „stufenweisen Kontrollverdichtung“ in Bezug auf die Kontrolle der IKT-Nutzung von Bediensteten nicht aufgegeben werden, nämlich, dass bei der Einleitung allgemeiner (vorerst anonymer) Kontrollmaßnahmen im ersten Schritt ein Rückschluss auf einzelne Bedienstete zu verhindern ist, indem auf Organisationseinheiten mit einer Mindestanzahl an Bediensteten abzustellen ist. Das ist nur dann gewährleistet, wenn zu einer kontrollierten Bediensteten-Gruppe mehr als fünf Personen zählen. Diese Anzahl gewährleistet statistisch (auch nach Ansicht der – ehemaligen – Datenschutzkommission [DSK], vgl deren Empfehlung vom 22.5.2013, GZ K213.180/0021-DSK/2013), dass ein Rückschluss auf bestimmte Personen nicht möglich ist. Die bisherige Regelung in § 79e Abs 4 BDG entspricht dieser Empfehlung der DSK (mit der Maßgabe, dass im Gesetzestext von „mehr“ statt „mindestens“ die Rede sein müsste). Nach Ansicht der BAK muss diese Zielrichtung gerade wegen der unionsrechtlichen Grundsätze der Datenminimierung und Verhältnismäßigkeit auch in Zukunft beibehalten werden. Nur nebenbei sei erwähnt, dass für die Aufdeckung einer gröblichen Dienstpflichtverletzung bei Vorliegen eines begründeten Verdachtes gegen einen bestimmten Beamten sowieso von der erwähnten (beizubehaltenden) Vorgabe gemäß § 79g Abs 7 BDG abgegangen werden kann.

Stellungnahmemöglichkeit von betroffenen Beamten/innen

Im geplanten § 79f Abs 5 BDG ist vorgesehen, der Beamtin oder dem Beamten, welche/r von Kontrollmaßnahmen betroffen ist, die sie/ihn betreffenden Daten des Protokolls zur Verfügung zu stellen sowie ist sie/er nach dem geplanten § 79g Abs 7 BDG umgehend über den Bericht der IT-Stelle und dem diesem vorausgegangenen Ermittlungsauftrag zu informieren. Diese Informationspflicht ist bereits in der derzeit geltenden Fassung der §§ 79f und 79g BDG enthalten und wird begrüßt, ist sie doch eine wesentliche Voraussetzung, damit betroffene Personen ihren Beitrag zu Klärung des Sachverhalts leisten können. In diesem Zusammenhang

soll daher nach Ansicht der BAK die Möglichkeit zur Abgabe einer Stellungnahme der betroffenen Beamtin/des betroffenen Beamten ebenfalls direkt im Gesetz normiert werden. Seitens der IT-Stelle sollen zumutbare Maßnahmen zu ergreifen sein, wenn damit die Angaben der Betroffenen gestützt werden können bzw um diese zu überprüfen. Diese beiden Maßnahmen dienen der Stärkung der Betroffenenrechte.

§ 280 Abs 1 und 2 neu:

Zweckbindungsaufhebung sowie zu weite Zweckdefinition überdenken

In § 280 Abs 1 neu wird angeführt, dass die personenbezogenen Daten (sowie die personenbezogenen Daten besonderer Kategorien) zu einem anderen in Abs 2 genannten Zweck, als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, verarbeitet werden dürfen. In den Erläuterungen wird zu dieser Ermächtigung ausgeführt, dass die Weiterverarbeitung zu einem anderen Zweck, der ebenso wie der ursprüngliche Zweck der Verarbeitung von Abs 2 umfasst sein muss, nur dann möglich ist, sofern die personenbezogenen Daten oder die personenbezogenen Daten besonderer Kategorien zu diesem „neuen" Zweck ebenfalls erhoben und verarbeitet werden dürften. Dass, sofern vorgenannte Voraussetzung zutrifft, eine neuerliche Erhebung aus Gründen der Verwaltungsvereinfachung, Kostenersparnis etc unterbleiben soll, ist für die BAK durchaus nachvollziehbar. Bedenklich ist jedoch, dass sich eben diese erforderliche konkrete und zu dokumentierende Prüfung der Rechtmäßigkeit und Verhältnismäßigkeit der Weiterverarbeitung nicht im Gesetzestext wiederfindet.

Verstärkt werden diese Bedenken überdies durch die Definition der Zwecke einer Verarbeitung, Übermittlung oder Weiterverwendung in den Z 1 bis 3 des geplanten § 280 Abs 2 BDG. Diese sind insgesamt gesehen sehr weitreichend formuliert und es ist für die Verarbeitung, Übermittlung oder Weiterverarbeitung von personenbezogenen Daten das Zutreffen eines Zwecks der angeführten Zwecke ausreichend. Nach Ansicht der BAK wäre insbesondere Z 1 konkreter zu fassen: Nach dem vorliegenden Entwurf dürfen Daten verarbeitet, übermittelt oder weiterverarbeitet werden, wenn dies für die Aufrechterhaltung oder das Funktionieren des Öffentlichen Dienstes erforderlich ist. Was nun darunter zu verstehen ist, bleibt offen. Nach Ansicht der BAK ist der Zweck nicht hinreichend konkret formuliert, um die Vorgaben nach Art 5 Abs 1 b) DS-GVO, wonach jeder Datenverarbeitung ein „festgelegter, eindeutiger und legitimer" Zweck zugrunde liegen muss, zu erfüllen.

§ 280a neu:

Anpassung der Aufbewahrungsfristen von Protokolldaten

Im Zusammenhang mit der Regelung der Fristen für die Aufbewahrung von Protokolldaten in den Abs 4 und 5 des geplanten § 280a BDG, welche bei lesenden Zugriffen drei Jahre, bei datenändernden Zugriffen sieben Jahre betragen bzw wonach laut Abs 7 des geplanten § 280a BDG durch Verordnung kürzere oder längere Fristen vorgesehen werden können, regt die BAK an, die Fristen für die Aufbewahrung von Protokolldaten generell an die Aufbewah-

rungsfristen/Löschfristen der zugrundeliegenden Daten anzupassen. Solange personenbezogene Daten und personenbezogene Daten besonderer Kategorien noch nicht gelöscht sind, sollte nach Ansicht der BAK auch jede vorgenommene Änderung oder Einsichtnahme nachvollzogen werden können.

§ 280b neu:

Gänzlichen Ausschluss von Betroffenenrechten überdenken

Die Abs 5 bis 8 im geplanten § 280b BDG sehen die Beschränkung der Rechte auf Berichtigung (Art 16 DS-GVO), der Löschung (Art 17 DS-GVO), Einschränkung der Verarbeitung (Art 18 DS-GVO) sowie des Widerspruchsrechts (Art 21 DS-GVO) vor. Die im Entwurf vorliegenden Beschränkungen erfüllen nach Ansicht der BAK nicht die strengen Voraussetzungen des Art 23 DS-GVO. Dieser gestattet zwar die Beschränkung von Betroffenenrechte durch Rechtsvorschriften der Mitgliedsstaaten vor, dies jedoch nur, wenn die Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet, es sich um eine in einer demokratischen Gesellschaft notwendigen und verhältnismäßige Maßnahme handelt, die Beschränkung einem der in Art 23 Abs 1 lit a-j DS-GVO genannten Zwecke dient und die Rechtsvorschrift die in Art 23 Abs 2 DS-GVO genannten Mindestinhalte aufweist.

Die Erläuternden Bemerkungen begründen den Schritt zusammengefasst mit einem überwiegenden schutzwürdigen öffentlichen Interesse daran. Ausnahmen von den Betroffenenrechten sollten aber nur im absolut erforderlichen Umfang vorgesehen werden, um zweifelsfrei dem Verhältnismäßigkeitsgrundsatz zu entsprechen. Nach Ansicht der BAK kann der generelle Ausschluss der wichtigsten Betroffenenrechte bei der Datenverarbeitung überschießend sein. So kann doch im Einzelfall der Nachweis von Betroffenen gelingen, dass seine Rechte schutzwürdiger sind. Durch einen pauschalen Ausschluss bleibt für derartige Abwägungen im Einzelfall kein Raum.

Abschließende Anmerkung: Umfassende Mitwirkungsrechte der Interessenvertretung müssen sichergestellt werden, um bei der Verarbeitung von personenbezogenen Daten die Schutzinteressen der Bediensteten zu wahren!

Der BAK ist es wichtig, dass die Rechte der Bediensteten, so auch ihre Datenschutzrechte und Persönlichkeitsrechte, gerade im Zusammenhang mit der voranschreitenden Digitalisierung der Arbeitswelt bzw im öffentlichen Dienst, ausreichend geschützt sind. Dies kann nur gelingen, wenn umfassende Mitwirkungsrechte ihrer Interessenvertretung sichergestellt sind, und zwar auf allen Ebenen und in allen Bereichen, wenn es um die Gestaltung des Einsatzes von technischen Systemen und Maßnahmen geht, die personenbezogene Daten und personenbezogene Daten besonderer Kategorien im Beschäftigungskontext verarbeiten.

Die BAK ersucht um Berücksichtigung ihrer Anregungen.

Rudi Kaske
Präsident
F.d.R.d.A.

Alice Kundtner
iV des Direktors
F.d.R.d.A.