2/2023
25 – 48

Aufhebung
§ 9 Abs 1 DSG
Eva Souhrada-Kirchmayer

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Digitale Signatur

Elektronische Identität für Personen und Unternehmen

Interview mit Markus Vesely, A-Trust

Österreichs elektronische Identität

Jan Hospes, Lisa Seidl, Andreas Czák

FAQ: Auskunftsantrag mit digitaler Signatur

FAQ: ID Austria im Unternehmen einsetzen

Viktoria Haidinger

Beauskunftung der konkreten Empfänger

Barbara Wagner

Kritische Auseinandersetzung mit EuGH, *Österreichische Post*

Janos Böszörmenyi

Zusammenspiel von DSGVO und Datenschutzrecht im TKG

Natalie Ségur-Cabanac

Checkliste Whistleblowing gemäß HSchG

Hans-Jürgen Pollirer

ISSN 2313-5409

dako.manz.at

MANZ

Hans-Jürgen Pollirer
Senior Management Consultant bei der Secur-Data Betriebsberatungs-GmbH

Checkliste Whistleblowing gemäß HSchG

Anwendungsbereich; Umsetzungsfristen; Dokumentationspflichten; Informationssicherheit; Sanktionen. Die Checkliste enthält Prüffragen, die bei der Umsetzung des HinweisgeberInnenschutzgesetzes (HSchG) zu beachten sind. Auch bei bereits implementierten Whistleblowingsystemen ist zu prüfen, ob sie den Bestimmungen des HSchG entsprechen.

Einleitung

Bereits in der Dako 2020/23 wurde das Thema Whistleblowing im Rahmen einer Checkliste behandelt. Diese basierte allerdings auf der RL (EU) 2019/1937 des EP und des Rates vom 23. 10. 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden.[1] Eine Umsetzung dieser RL, die durch die MS spätestens bis zum 17. 12. 2021 erfolgen hätte sollen, lag in Österreich zum Zeitpunkt der Veröffentlichung dieser Checkliste allerdings noch nicht vor. Mit mehr als einjähriger Verspätung haben nun der NR am 1. 2. 2023 und der BR am 16. 2. 2023 das neue HinweisgeberInnenschutzgesetz (HSchG) mit anschließenden Gesetzesänderungen beschlossen; mit 24. 2. wurde es im BGBl I 2023/6[2] veröffentlicht. Dies allerdings gegen die Stimmen der Opposition, welche die Bestimmungen für unzureichend halten. So seien außerhalb der RL nur einzelne innerstaatliche Straftaten umfasst, nicht aber etwa Betrug oder Veruntreuung sowie Mobbing, Diskriminierung, Menschenhandel oder Untreue.

Ziel des HSchG

Ziel des HSchG ist es, Personen, die Informationen über rechtlich fragwürdige Praktiken in ihrem beruflichen Umfeld weitergeben, vor Repressalien am Arbeitsplatz und anderen negativen Konsequenzen sowie existenzbedrohenden Gerichtsprozessen zu schützen. So enthält § 20 den Schutz vor Vergeltungsmaßnahmen gegen Hinweisgeberinnen und Hinweisgeber und der Personen in ihrem Umkreis. Ua sind Suspendierung, Kündigung, Gehaltskürzungen, Disziplinarmaßnahmen, Versagung einer Beförderung explizit verboten.

Anwendungsbereich

Das HSchG ist auf Hinweise zu Rechtsverletzungen in Unternehmen und juristischen Personen des öffentlichen Sektors mit jeweils 50 oder mehr Arbeitnehmern/Bediensteten anzuwenden. Gem § 3 Abs 3 HSchG gilt das für Hinweise zu **Verstößen in den Bereichen**

1. Öffentliches Auftragswesen;
2. Finanzdienstleistungen, Finanzprodukte und Finanzmärkte sowie Verhinderung von Geldwäsche und Terrorismusfinanzierung;
3. Produktsicherheit und -konformität;
4. Verkehrssicherheit;
5. Umweltschutz;
6. Strahlenschutz und nukleare Sicherheit;
7. Lebensmittel- und Futtermittelsicherheit, Tiergesundheit und Tierschutz;
8. öffentliche Gesundheit;
9. Verbraucherschutz;
10. Schutz der Privatsphäre und personenbezogener Daten sowie Sicherheit von Netz- und Informationssystemen;
11. Verhinderung und Ahndung von Straftaten nach den §§ 302 bis 309 StGB.

Punkt 11 behandelt zusätzlich zu den in der RL (EU) 2019/1937 enthaltenen Rechtsbereichen im Bereich der Beamten und Amtsträger sowie Schiedsrichter (Mitglieder von Schiedsgerichten) den Missbrauch der Amtsgewalt (§ 302), die fahrlässige Verletzung der Freiheit der Person oder des Hausrechts (§ 303), Bestechlichkeit (§ 304), Vorteilsannahme (§ 305), Vorteilsannahme durch Beeinflussung (§ 306), Bestechung (§ 307), Vorteilszuwendung (§ 307a), Vorteilszuwendung durch Beeinflussung (§ 307b), verbotene Intervention (§ 308) sowie Geschenkannahme und Bestechung von Bediensteten oder Beauftragten (§ 309).

Weiters sind Rechtsverletzungen zum Nachteil der finanziellen Interessen der EU sowie die Verletzung von Binnenmarktvorschriften und der Körperschaftsteuervorschriften umfasst.

[1] https://kurzelinks.de/6evq [2] www.ris.bka.gv.at/eli/bgbl/i/2023/6

Umsetzung des HSchG

Normadressaten des neuen HSchG sind sowohl Einrichtungen des öffentlichen Sektors als auch private Unternehmen und gemeinnützige Einrichtungen und Vereine, sofern sie mindestens 50 Mitarbeiterinnen und Mitarbeiter beschäftigen. Unabhängig von der Anzahl der Mitarbeiterinnen und Mitarbeiter sind gem § 3 Abs 2 HSchG auch bestimmte Branchen verpflichtet, einen **internen Meldekanal** zu implementieren. Diese Verpflichtung bezieht sich auf Art 8 Abs 4 der RL (EU) 2019/1937 und betrifft insb Unternehmen des Finanzdienstleistungssektors wie zB die Bilanzbuchhaltungsberufe, Versicherungsmakler, Vermögensberater, Wertpapiervermittler, Immobilienmakler uÄ.

Alle Adressaten sind verpflichtet, eine **interne Meldestelle** einzurichten, wobei konkrete Vorgaben über die Ausgestaltung im HSchG nicht enthalten sind. Gem § 13 HSchG müssen jedoch gewisse Voraussetzungen erfüllt sein, zB die Bereitstellung der notwendigen finanziellen oder personellen Mittel sowie die Möglichkeit zur unparteiischen Prüfung von Hinweisen auf ihre Stichhaltigkeit. Hinweise müssen der internen Stelle schriftlich, mündlich oder in beiden Formen mitgeteilt werden können, insb müssen auch anonyme Hinweise möglich sein.

Gem § 11 Abs 1 HSchG müssen Hinweisgeberinnen und Hinweisgeber dazu angeregt werden, die Abgabe von Hinweisen an die interne Stelle gegenüber externen Stellen zu bevorzugen. Als **externe Stelle** ist zur Entgegennahme und Behandlung von Hinweisen für Rechtsträger des privaten Sektors oder des öffentlichen Sektors gem § 15 Abs 1 HSchG das Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung zuständig.

Arbeitsrechtliche Aspekte

Da idR die Mehrheit der Hinweisgeberinnen und Hinweisgeber Arbeitnehmerinnen und Arbeitnehmer sein werden, stellt sich auch die Frage, inwieweit der **Betriebsrat** (BR) in die Umsetzung des Whistleblowingsystems (kurz: WBS) **einzubeziehen** ist. Zu dieser Thematik gibt es im HSchG keinerlei Hinweise. Entspricht das implementierte WBS den Bestimmungen des HSchG, so ist nach mM idR der Abschluss einer Betriebsvereinbarung (BV) entbehrlich, da eine gesetzliche Verpflichtung zur Einrichtung eines WBS aufgrund des HSchG besteht. Nur wenn die Hinweismöglichkeiten des WBS über die vom HSchG umfassten und dort abschließend angeführten Bereiche hinausgehen und die Menschenwürde berühren, wird der Abschluss einer BV notwendig sein. Jedenfalls wird anhand des geplanten WBS fallweise evaluiert werden müssen, ob ein Mitbestimmungsrecht des BR vorliegt.

Umsetzungsfristen

Wie nachfolgend gezeigt, sind die Umsetzungsfristen für die Implementierung des WBS sehr knapp bemessen. Entsprechende Umsetzungsmaßnahmen müssen daher sowohl im öffentlichen Sektor wie auch von privaten Unternehmen, gemeinnützigen Einrichtungen und Vereinen relativ rasch eingeleitet werden:

Unternehmen und juristische Personen des öffentlichen Sektors

- ab 250 Arbeitnehmern: bis (spätestens) 25. 8. 2023
- von 50 bis 249 Arbeitnehmern: bis (spätestens) 17. 12. 2023

Dokumentationspflichten

Gem § 9 HSchG sind von internen und externen Stellen alle eingehenden Hinweise zu dokumentieren. Ihr Eingang ist den Hinweisgeberinnen und Hinweisgebern unverzüglich, spätestens aber innerhalb von sieben Tagen zu bestätigen. Erfolgt der Hinweis mündlich, so sind die Stellen nach Zustimmung der Hinweisgeberinnen und Hinweisgeber berechtigt, Tonaufzeichnungen oder Transkriptionen des Gesprächs anzufertigen.

Datenschutzrechtliche Aspekte

Als **Verantwortliche** iSd Art 4 Z 7 DSGVO gelten die jeweiligen Behörden bzw Unternehmen. Hinweisgeberinnen und Hinweisgeber gelten nur dann als Verantwortliche, wenn sie personenbezogene Daten verarbeiten, die über das erforderliche Ausmaß für die Verfolgung des Hinweises hinausgehen. Insb wird der Grundsatz der Datenminimierung des Art 5 Abs 1 lit c DSGVO zu beachten sein.

Bei gemeinsamem Betrieb eines WBS innerhalb einer **Konzerngesellschaft** sind diese gemeinsame Verantwortliche iSd Art 26 DSGVO.

Entspricht das implementierte WBS den Bestimmungen des HSchG, dann dient dieses iVm Art 6 Abs 1 lit c DSGVO als **Rechtsgrundlage.** Geht das WBS über die Rechtsbereiche des HSchG hinaus, kann die Datenverarbeitung gegebenenfalls auf das berechtigte Interesse des Verantwortlichen iSd Art 6 Abs 1 lit f DSGVO – allerdings erst nach einer Abwägung mit den Interessen des Betroffenen, die zugunsten des Verantwortlichen ausfällt – gestützt werden.

Grundsätzlich benötigt ein WBS, das den Bestimmungen des HSchG entspricht, **keine DSFA** gem Art 35 DSGVO, da der Gesetzgeber eine solche gem Art 35 Abs 10 und ErwGr 92 bereits auf abstrakter Ebene durchgeführt hat. Nur wenn das WBS über den Rechtsbereich des HSchG hinausgeht, wird eine DSFA durchzuführen sein.

Nach den Bestimmungen des § 8 Abs 9 HSchG **entfallen** folgende in der DSGVO normierte **Betroffenenrechte,** allerdings nur so lange und insoweit dies zum Schutz der Identität einer Hinweisgeberin oder eines Hinweisgebers oder zum Erreichen der Zwecke des WBS erforderlich ist:

- Recht auf Information (§ 43 DSG; Art 13, 14 DSGVO);
- Recht auf Auskunft (§ 1 Abs 3 Z 1, § 44 DSG; Art 15 DSGVO);
- Recht auf Berichtigung (§ 1 Abs 3 Z 2, § 45 DSG; Art 16 DSGVO);
- Recht auf Löschung (§ 1 Abs 3 Z 2, § 45 DSG; Art 17 DSGVO);
- Recht auf Einschränkung der Verarbeitung (§ 45 DSG; Art 18 DSGVO);
- Widerspruchsrecht (Art 21 DSGVO) sowie
- Recht auf Benachrichtigung von einer Verletzung des Schutzes personenbezogener Daten (§ 56 DSG; Art 34 DSGVO).

Die Unternehmen und juristischen Personen des öffentlichen Sektors haben aber sicherzustellen, dass Hinweisgeberinnen und Hinweisgeber sowie zusätzliche Personen, die von § 2 HSchG umfasst sind, Zugang zu Informationen über das implementierte WBS erhalten. Am besten wird das durch eine Information auf der Website sichergestellt werden können.

§ 8 Abs 11 HSchG sieht nun eine fünfjährige **Aufbewahrungsfrist** für personenbezogene Daten ab ihrer letzten Verarbeitung oder Übermittlung vor, während der ME noch eine dreißigjährige Aufbewahrungsfrist normierte. Nach § 8 Abs 12 HSchG sind durchgeführte Verarbeitungsvorgänge wie insb Änderungen, Abfragen und Übermittlungen zu protokollieren und drei Jahre nach Entfall der Aufbewahrungsfrist gem Abs 11 zu löschen.

Informationssicherheitstechnische Aspekte

Informationssicherheitstechnische Aspekte werden im HSchG nur rudimentär angesprochen. So enthält § 7 Abs 1 HSchG die Forderung, dass die Identität von Hinweisgeberinnen und Hinweisgebern durch die Meldestelle zu schützen ist. Weites enthält § 11 Abs 1 HSchG die Forderung, dass das WBS technisch und organisatorisch den Bestimmungen des Art 25 DSGVO entsprechen muss. Gem § 16 Abs 3 HSchG, der die Eignung der Meldekanäle externer Stellen regelt, müssen WBS den Schutz der Identität von Hinweisgebern und Hinweisgeberinnen sowie der von einem Hinweis betroffenen Personen, die Vertraulichkeit, den Datenschutz und die Verwendung standardisierter, dem Stand der Technik entsprechender Soft- und Hardware für das WBS gewährleisten.

Sanktionen

Die (versuchte) Behinderung von Hinweisgeberinnen und Hinweisgebern iZm einer Hinweisgebung, die Setzung der in § 20 HSchG genannten Maßnahmen zur Vergeltung der Hinweisgebung, die Verletzung der Vertraulichkeit oder die wissentliche Abgabe eines falschen Hinweises wird mit einer **Verwaltungsstrafe** bis zu € 20.000,– bzw im Wiederholungsfall mit bis zu € 40.000,– sanktioniert.

Für die Nichteinrichtung von internen Meldekanälen sieht das HSchG **allerdings keine Sanktion vor**.

Die Checkliste enthält Prüffragen, die Sie bei der Umsetzung des HSchG unterstützen sollen. Auch für Unternehmen, die bereits ein WBS eingeführt haben, ist die eine oder andere Prüffrage sicher von Interesse. Va wird bei bereits implementierten WBS zu prüfen sein, ob sie den Bestimmungen des HSchG entsprechen und welche zusätzlichen Maßnahmen zu treffen sind, wenn dies nicht der Fall ist.

Prüffragen

Prüffrage	ja	nein
Frage 1: Sind in Ihrem Unternehmen die notwendigen Voraussetzungen für die Einführung eines WBS gegeben? ***Anmerkung:*** *Voraussetzung für die erfolgreiche Einführung eines WBS ist es, Vorbehalte der Mitarbeiterinnen und Mitarbeiter auszuräumen und ihnen zu erklären, dass Sinn und Zweck dieser Maßnahme nicht die ungefilterte Verdächtigung anderer Personen ist („Vernadern"), sondern das Aufdecken schwerwiegender Missstände im Unternehmen. Es ist idZ unbedingt notwendig, frühzeitig zentrale Stakeholder wie das Management, die Personalabteilung, das Marketing, die IT-Abteilung, den BR und auch den DSBA (Datenschutzbeauftragten) in den Entscheidungsprozess vor Einführung eines WBS einzubinden.*		
Frage 2: Wurde vor Einführung des WBS geprüft, ob eine entsprechende Rechtsgrundlage vorliegt? ***Anmerkung:*** *Entspricht das WBS den Bestimmungen des HSchG, dann dient dieses iVm Art 6 Abs 1 lit c DSGVO als Rechtsgrundlage. Wenn das WBS zusätzlich Rechtsbereiche abdeckt, die vom HSchG nicht umfasst sind, kann die Datenverarbeitung auf das berechtigte Interesse des Verantwortlichen gem Art 6 Abs 1 lit f DSGVO gestützt werden; dies allerdings erst nach einer Abwägung mit den Interessen des Betroffenen, die zugunsten des Verantwortlichen ausfällt, und unter Beachtung der arbeitsrechtlichen Bestimmungen.*		
Frage 3: Wurde vor Einführung des WBS eine BV abgeschlossen bzw bei Nichtvorhandensein eines BR die Einwilligung aller Mitarbeiterinnen und Mitarbeiter eingeholt? ***Anmerkung:*** *Entspricht das WBS den Bestimmungen des HSchG, so ist nach mM idR der Abschluss einer BV nicht notwendig, da eine gesetzliche Verpflichtung zur Einrichtung eines solchen Systems besteht. Geht das Meldesystem jedoch über das HSchG hinaus und wird die Menschenwürde berührt, so ist das Mitwirkungsrecht des BR (insb §§ 96ff ArbVG) zu beachten und eine BV abzuschließen.* *Grundsätzlich kommen folgende Formen einer BV in Frage:* ■ ***§ 96 Abs 1 Z 3 ArbVG:*** *Wird das WBS als Kontrollmaßnahme eingesetzt, welche die Menschenwürde berührt – das wird bei den meisten WBS der Fall sein –, so hat der BR de facto ein Vetorecht gegen die Implementierung des Systems und seine Zustimmung im Rahmen einer BV ist für die Rechtswirksamkeit dieser Maßnahme erforderlich.* ■ ***§ 96a Abs 1 Z 1 ArbVG:*** *Ist das WBS mit automationsunterstützter Datenerfassung, -verarbeitung bzw -weitergabe verknüpft, so bedarf es ebenfalls der Zustimmung des BR. Diese kann jedoch durch die Entscheidung der Schlichtungsstelle ersetzt werden.* ■ ***§ 97 Abs 1 Z 1 ArbVG:*** *Diese Norm bietet die Rechtsgrundlage für allgemeine Ordnungsvorschriften, die das Verhalten im Betrieb regeln, und erfordert den Abschluss einer erzwingbaren BV.* *Bei Unternehmen, die über keinen BR verfügen und in denen somit der Abschluss einer BV gem § 96 Abs 1 Z 3 ArbVG nicht möglich ist, ist das Recht jedes einzelnen Mitarbeiters und jeder einzelnen Mitarbeiterin zu beachten und gem § 10 Abs 1 AVRAG die Einwilligung jedes einzelnen Mitarbeiters und jeder einzelnen Mitarbeiterin einzuholen.*		
Frage 4: Wurde der DSBA frühzeitig über die Einführung des WBS informiert? ***Anmerkung:*** *Dem DSBA kommt die Aufgabe zu, vor Inbetriebnahme des WBS die Einhaltung der datenschutzrechtlichen Grundsätze zu prüfen. Insb wird er zu prüfen haben, ob die Durchführung einer DSFA erforderlich ist.*		
Frage 5: Wird für den Betrieb des WBS ein externer Dienstleister eingesetzt? ***Anmerkung:*** *Wird ein externer Dienstleister teilweise oder zur Gänze mit dem Betrieb des WBS betraut, dann ist nach den Bestimmungen des Art 28 DSGVO eine Auftragsverarbeitungsvereinbarung abzuschließen.*		
Frage 6: Wird das WBS von mehreren Unternehmen gemeinsam betrieben? ***Anmerkung:*** *Soweit Verantwortliche iSd Art 4 Z 7 DSGVO ein WBS gemeinsam betreiben, so sind sie nach den Bestimmungen des § 8 Abs 4 Z 4 HSchG gemeinsam Verantwortliche iSd Art 26 DSGVO.*		
Frage 7: Wird ein WBS eingesetzt, das bereits vor der Geltung der DSGVO einer Vorabkontrolle der DSB unterzogen wurde? ***Anmerkung:*** *In diesem Fall ist die Durchführung einer DSFA entbehrlich.*		
Frage 8: Wurde vor dem Einsatz des WBS eine DSFA durchgeführt? ***Anmerkung:*** *Die Durchführung einer DSFA ist nur dann notwendig, wenn das WBS über die Rechtsbereiche des HSchG hinausgeht.*		
Frage 9: Wird der Personenkreis, der für die Nutzung des WBS in Frage kommt, über das Verfahren angemessen informiert? ***Anmerkung:*** *Der für die Nutzung des WBS in Frage kommende Personenkreis wird in § 2 HSchG definiert und hat gem § 10 HSchG einfachen Zugang zu klaren Informationen über das WBS zu erhalten. Am besten wird das durch eine Information auf der Website sichergestellt werden können. Der Mindestinhalt einer solchen Information kann § 10 Abs 2 HSchG entnommen werden.*		
Frage 10: Enthält die Information über das WBS eine klare Definition der meldefähigen Verstöße und wurden diese entsprechend kommuniziert? ***Anmerkung:*** *Neben dem in § 3 HSchG definierten „sachlichen Geltungsbereich" könnten uU auch noch andere für das Unternehmen relevante Inhalte definiert werden. Dabei sind mögliche Auswirkungen auf das Erfordernis einer DSFA sowie auf die arbeitsrechtlichen Bestimmungen zu beachten.*		

Prüffrage	ja	nein
Frage 11: Enthält die Information über das WBS eine klare Festlegung der zulässigen Hinweisgeberinnen und Hinweisgeber? ***Anmerkung:*** *§ 2 HSchG enthält eine detaillierte Aufzählung jener Personen, die vom Geltungsbereich umfasst sind. Das sind generell Personen, die aufgrund beruflicher Verbindung zu einem Rechtsträger des privaten oder des öffentlichen Sektors Informationen über Rechtsverletzungen erlangt haben.*		
Frage 12: Werden die Hinweisgeberinnen und Hinweisgeber angeregt, für ihre Hinweise die interne Meldestelle und nicht externe Meldestellen zu wählen? ***Anmerkung:*** *§ 11 HSchG fordert, dass WBS in einer Weise einzurichten sind, die Hinweisgeberinnen und Hinweisgeber zur Bevorzugung der internen Meldestelle anregt.*		
Frage 13: Wird die Identität der Hinweisgeberinnen und Hinweisgeber durch die internen und externen Stellen entsprechend geschützt? ***Anmerkung:*** *§ 7 Abs 1 HSchG fordert den Schutz der Identität von Hinweisgeberinnen und Hinweisgeber durch die internen und externen sowie die mit den Aufgaben der internen Stelle beauftragten Stellen während des Untersuchungsprozesses. Dieser Schutz kann durch entsprechende IT-Sicherheitsmaßnahmen wie ein flexibles Rechte- und Rollenprinzip, datenschutzkonforme Pseudonymisierung und Anonymisierung sowie durch entsprechende Arbeitsanweisungen an die Mitarbeiterinnen und Mitarbeiter der internen und externen Stellen erreicht werden.*		
Frage 14: Wurde geregelt, unter welchen Umständen die Identität der Hinweisgeberin oder des Hinweisgebers offengelegt werden darf? ***Anmerkung:*** *Nach den Bestimmungen des § 7 Abs 3 HSchG darf die Identität der Hinweisgeberinnen und Hinweisgeber nur dann offengelegt werden, wenn eine Verwaltungsbehörde, ein Gericht oder die Staatsanwaltschaft diese im Rahmen eines verwaltungsbehördlichen oder gerichtlichen Verfahrens oder eines Ermittlungsverfahrens nach der StPO für unerlässlich hält, wobei die Verhältnismäßigkeit dieser Maßnahme zu prüfen ist. Sollen Daten der Hinweisgeberin oder des Hinweisgebers offengelegt werden, so sind diese gem § 7 Abs 4 HSchG von der Behörde vor der Offenlegung zu unterrichten.*		
Frage 15: Ist sichergestellt, dass Hinweise, die offenkundig falsch gegeben werden, im Rahmen des WBS zurückgewiesen werden? ***Anmerkung:*** *§ 6 Abs 4 HSchG fordert die Zurückweisung von offenkundig falschen Hinweisen sowie eine nachrichtliche Meldung an die Hinweisgeberin oder den Hinweisgeber mit einem Hinweis auf mögliche Schadenersatzansprüche, die in § 24 HSchG normiert sind. Nach den Bestimmungen des § 9 Abs 1 HSchG ist jedoch jeder Hinweis auf seine Stichhaltigkeit zu prüfen.*		
Frage 16: Ermöglicht der Meldekanal die Abgabe der Hinweise in schriftlicher und/oder mündlicher Form? ***Anmerkung:*** *Die Art des Meldekanals wird den Unternehmen nicht exakt vorgeschrieben. Gem § 13 Abs 5 HSchG müssen die Hinweise der internen Stelle aber schriftlich oder mündlich oder in beiden Formen gegeben werden können, auch anonyme Hinweise müssen möglich sein. Grundsätzlich gibt es* ***fünf verschiedene Meldekanäle,*** *und zwar:* ■ **Briefkasten:** Aufstellung eines Briefkastens im Unternehmen, in den Hinweisgeber Meldungen einwerfen können. ■ **E-Mail:** Einrichtung eines zentralen E-Mailkontos, an das Hinweise gesendet werden können. ■ **Ombudsmann:** Bestellung einer externen Person (in der Regel ein Anwalt), der als Anlaufstelle für Hinweisgeber und Hinweisgeberinnen dient. ■ **Telefon:** Einrichtung einer zentralen Telefonnummer, unter der Hinweise abgegeben werden können. ■ **Digitales WBS:** Einrichtung einer Onlineplattform für Hinweisgeber und Hinweisgeberinnen. *Der Leitfaden für die Einführung von Hinweisgebersystemen der EQS-Group[3] bietet eine sehr gute Gegenüberstellung der Vor- und Nachteile der einzelnen Meldekanäle.*		
Frage 17: Ist die interne Stelle mit den zur Erfüllung ihrer Aufgaben notwendigen finanziellen und personellen Mitteln ausgestattet? ***Anmerkung:*** *Diese Forderung entspricht § 13 Abs 1 HSchG. Als interne Stelle wird gem § 5 Z 6 HSchG jene Person oder Abteilung oder sonstige Organisationseinheit innerhalb eines Unternehmens oder einer juristischen Person des öffentlichen Sektors bezeichnet, die Hinweise entgegennimmt, überprüft sowie im Hinblick auf Folgemaßnahmen oder sonst weiter behandelt.*		
Frage 18: Ist durch die interne Meldestelle die Entgegennahme und Behandlung von Hinweisen unparteilich und unvoreingenommen sichergestellt und erfolgt die Bestätigung des Eingangs der Meldung unverzüglich, spätestens jedoch nach 7 Kalendertagen? ***Anmerkung:*** *Nach den Bestimmungen des § 13 Abs 2 HSchG sind jedenfalls Vorkehrungen zu treffen, um internen Stellen die weisungsfreie Erledigung der Hinweise zu ermöglichen. § 9 Abs 1 HSchG fordert eine schriftliche Bestätigung des Eingangs des Hinweises an die Hinweisgeberin oder den Hinweisgeber unverzüglich, jedoch spätestens nach 7 Kalendertagen.*		
Frage 19: Ist sichergestellt, dass auf Ersuchen einer Hinweisgeberin oder eines Hinweisgebers eine Zusammenkunft zur Besprechung des Hinweises stattfinden kann? ***Anmerkung:*** *§ 13 Abs 5 HSchG fordert, dass derartigen Ersuchen einer Hinweisgeberin oder eines Hinweisgebers innerhalb von 14 Kalendertagen zu entsprechen ist.*		
Frage 20: Ist sichergestellt, dass Hinweisgeberinnen und Hinweisgeber ihre Hinweise ergänzen oder berichtigen können? ***Anmerkung:*** *Diese Forderung ergibt sich aus den Bestimmungen des § 13 Abs 8 HSchG. Auf Verlangen ist die Entgegennahme von Ergänzungen oder Berichtigungen spätestens nach 7 Kalendertagen schriftlich zu bestätigen.*		
Frage 21: Ist eine Rückmeldung an die Hinweisgeberin und den Hinweisgeber, welche Maßnahmen ergriffen worden sind, innerhalb angemessener Zeit möglich? ***Anmerkung:*** *§ 13 Abs 9 HSchG fordert, dass spätestens 3 Monate nach Entgegennahme eines Hinweises die Hinweisgeberin oder der Hinweisgeber darüber zu informieren ist, welche Folgemaßnahmen ergriffen wurden bzw aus welchen Gründen der Hinweis nicht weiterverfolgt wird.*		
Frage 22: Ist sichergestellt, dass personenbezogene Daten, die für die Bearbeitung eines Hinweises nicht benötigt werden, unverzüglich gelöscht werden? ***Anmerkung:*** *Nach den Bestimmungen des § 8 Abs 10 HSchG dürfen Daten, die zur Bearbeitung eines Hinweises nicht benötigt werden, nicht erhoben werden bzw sind unverzüglich zu löschen, falls sie unbeabsichtigt erhoben wurden.*		
Frage 23: Ist die fünfjährige Aufbewahrungsfrist für personenbezogene Daten sichergestellt? ***Anmerkung:*** *Nach den Bestimmungen des § 8 Abs 11 HSchG sind die personenbezogenen Daten ab ihrer letztmaligen Verarbeitung oder Übermittlung fünf Jahre und darüber hinaus so lange aufzubewahren, wie sie zur Durchführung bereits eingeleiteter verwaltungsbehördlicher oder gerichtlicher Verfahren oder eines Ermittlungsverfahrens nach der StPO erforderlich sind. Nach Ablauf der Aufbewahrungsfrist sind diese Daten unverzüglich zu löschen.*		

[3] https://www.integrityline.com/de/knowhow/white-paper/hinweisgeberschutz-fuer-unternehmen/

Prüffrage	ja	nein
Frage 24: Werden Verarbeitungsvorgänge protokolliert? ***Anmerkung:*** *§ 8 Abs 12 HSchG fordert die Protokollierung durchgeführter Verarbeitungsvorgänge wie insb Änderungen, Abfragen und Übermittlungen sowie die Aufbewahrung dieser Protokolle bis 3 Jahre nach Entfall der fünfjährigen Aufbewahrungspflicht (s Frage 23).*		
Frage 25: Ist die Dokumentation von mündlichen Hinweisen gewährleistet? ***Anmerkung:*** *§ 9 Abs 2 HSchG erlaubt – bei Zustimmung der Hinweisgeberin oder des Hinweisgebers – die Tonaufzeichnung eines mündlich abgegebenen Hinweises oder eine Transkription des Gesprächs. Nach Möglichkeit ist der Hinweisgeberin und dem Hinweisgeber Gelegenheit zu geben, das Transkript zu prüfen und zu berichtigen.*		
Frage 26: Kann der Hinweisgeber oder die Hinweisgeberin über ein personalisiertes Log-in auf das WBS zugreifen? ***Anmerkung:*** *Die Anmeldemethode zum WBS und die zugehörigen Sicherheitsmaßnahmen müssen dem Schutzbedarf der übermittelten Inhalte angepasst werden. Weiters muss sichergestellt sein, dass durch Abfragen zur Authentifizierung nicht die Anonymität des Hinweisgebers und der Hinweisgeberin aufgehoben wird.*		
Frage 27: Ermöglicht der gewählte Meldekanal dem Hinweisgeber, Bilder, Videos oder Textdateien zu übermitteln? ***Anmerkung:*** *Je nach Art des Hinweises kann es notwendig sein, dass der Hinweisgeber und die Hinweisgeberin über die Meldung des entdeckten Missstandes hinaus ergänzende Materialien wie Dateien und Dokumente übermitteln muss.*		
Frage 28: Ist im Rahmen des WBS die rechtskonforme Information der beschuldigten Personen sichergestellt? ***Anmerkung:*** *Wenn personenbezogene Daten ohne Wissen der betroffenen Person (idF Beschuldigte) erhoben werden, so haben diese gem Art 14 DSGVO das Recht auf Information. Diese Informationspflicht kann allerdings nach den Bestimmungen des § 8 Abs 9 HSchG unterbleiben, wenn sie die Klärung und Verfolgung des aufgezeigten Missstandes gefährden würde. Diese Feststellung gilt auch in Bezug auf andere Betroffenenrechte wie Auskunft, Berichtigung, Löschung, Einschränkung und Widerspruch sowie die Benachrichtigung bei einem Data Breach.*		
Frage 29: Enthält das WBS auch ein integriertes Fallmanagement-System (Case Management System)? ***Anmerkung:*** *Das Fallmanagement-System sollte einfach zu bedienen sein und Funktionen bieten, die vom Empfang der Meldung über die Bearbeitung bis zur Verwaltung von Bearbeitungsvorgängen reichen. Es sollte weiters den Dialog zwischen dem Hinweisgeber oder der Hinweisgeberin und dem Fallmanager (Bearbeiter der Meldung) unterstützen.*		
Frage 30: Verfügt das eingesetzte WBS über eine Sicherheitszertifizierung? ***Anmerkung:*** *Ein WBS, das zB über eine ISO-27001-Zertifizierung verfügt, gewährleistet idR auch ausreichende Datensicherheit.*		

Dako 2023/21

Zum Thema

Über den Autor

Prof. KommR Hans-Jürgen Pollirer ist Senior Management Consultant bei der Secur-Data Betriebsberatungs-GmbH und fachkundiger Laienrichter für Datenschutz am BVwG sowie juristischer und technischer EuroPriSe-Gutachter. E-Mail: hj.pollirer@secur-data.at

Literatur

- *Aigner*, Magisterarbeit „Whistleblowing in Österreich“ (2011), http://othes.univie.ac.at/17347/1/2011-12-07_0948255.pdf;
- *Aschauer*, Whistleblowing im Arbeitsrecht (2012);
- *Grünanger/Goricnik* (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle² (2018)
- *Hauser/Bretti-Rainalter/Blumer*, Whistleblowing Report 2021 (2021), www.integrityline.com/de/knowhow/white-paper/whistleblowing-report/;
- *EDPS*, Leitlinien zur Verarbeitung personenbezogener Daten im Rahmen eines Verfahrens zur Meldung von Missständen (2019); https://edps.europa.eu/system/files/2021-07/19-12-17_whisteblowing_guidelines_en_195_de.pdf;
- *Gruber/M. Raschauer* (Hrsg), Whistleblowing (2015).