

Datenschutz-Folgeabschätzung zur Einführung eines Hinweisgebersystems

1. Zieldefinition

Ziel der Datenschutz-Folgeabschätzung (nachfolgend „**DSFA**“) ist die Herleitung von Maßnahmen zur Eingrenzung des Risikos bei risikoträchtigen Verarbeitungstätigkeiten. Die Dokumentation von der konkreten Tätigkeit und daraus erwachsenen Risiken ist mithin kein Selbstzweck, sondern Mittel zur Erreichung des vorgenannten Ziels und erfolgt deshalb auch aus anderem Blickwinkel, bzw. in anderer Detailtiefe. Während also eine vorausgegangene Analyse zum Risiko anhand von abstrakten Kriterien lediglich der Klärung der Frage diene, ob eine DSFA erforderlich ist, erfolgt nun die vertiefte Betrachtung des Risikos in der konkreten Form der Verarbeitungstätigkeit bei der Wilhelm Bötzel GmbH & Co. KG zur Klärung der Frage, welche Maßnahmen das Risiko begrenzen können.

2. Einleitung

Die Wilhelm Bötzel GmbH & Co. KG plant, das digitale Hinweisgebersystem (nachfolgend „**HWGS**“) der Aderhold Rechtsanwaltsgesellschaft mbH (nachfolgend „**Aderhold GmbH**“) in der jeweils geltenden Version einzuführen. Mithilfe des HWGS der Aderhold GmbH beabsichtigt die Wilhelm Bötzel GmbH & Co. KG eine Whistleblower-Kontaktmöglichkeit anzubieten, über die Mitarbeiter oder externe Personen vertrauensvoll und ohne notwendigerweise ihre Identität zu offenbaren, auf ein Fehlverhalten hinweisen können. Die Systembeschreibung des HWGS ergibt sich aus der nachfolgenden Darstellung:

- Die Hinweisgeber-Kontaktmöglichkeit auf der HWGS-Webseite ermöglicht es der hinweisgebenden Person, dort der Wilhelm Bötzel GmbH & Co. KG, einen Sachverhalt schriftlich mitzuteilen. Dabei erfährt die Wilhelm Bötzel GmbH & Co. KG nicht die Identität des Hinweisgebers¹, wenn diese nicht gewünscht und ausdrücklich mitgeteilt wird. In manchen Fällen wird es jedoch aus dem dargelegten Lebenssachverhalt nicht möglich sein, dass der Meldende anonym bleibt, weil sich die Identität hieraus bereits ergibt.
- Auf der HWGS-Webseite kann der Meldende folgende Angaben machen:
 - „In welche Kategorie fällt der Vorfall, den Sie melden?“ (Mögliche Auswahl: Finanzen; Datenschutz und IT-Sicherheit; Personal; Andere; Lieferkette; Diskriminierung/Ungleichbehandlung)
 - „Persönliche Informationen“ (offene Meldung oder anonyme Meldung)
 - „Bitte beschreiben Sie den Vorfall so genau und ausführlich wie möglich.“ (Angabe im Freitextfeld);
 - „Wo ist der Vorfall passiert?“ (Angabe im Freitextfeld);

¹ Aus Gründen der besseren Lesbarkeit wird im Folgenden auf die gleichzeitige Verwendung weiblicher und männlicher Sprachformen verzichtet und das generische Maskulinum verwendet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

- „Wann ist der Vorfall passiert?“ (Auswahl des Datums im Kalender-Menü) (Erläuterungen: „Wenn Sie sich nicht an den genauen Tag erinnern oder sich der Vorfall mehrfach wiederholt hat, können Sie dies später ergänzen. Geben Sie hier das Datum des Vorfalls an, an das Sie sich ungefähr erinnern. Sie können dieses Feld auch leer lassen.“);
- „Wer waren die beteiligten Personen?“ (Angaben im Freitextfeld)
- „Das Meldesystem wird von der Wilhelm Bötzel GmbH & Co. KG verwaltet. Bezieht sich diese Meldung auf Personen, die derzeit mit oder für die Wilhelm Bötzel GmbH & Co. KG arbeiten oder dies früher getan haben? (Mögliche Auswahl: Ja /Nein
- „Welche Beziehung besteht zwischen der Wilhelm Bötzel GmbH & Co. KG und der eigenen Person“ (Mögliche Auswahl: (Freier) Mitarbeiter, Lieferant/Dienstleister, Kunde, Sonstige);
- „Gibt es ergänzende Informationen?“ (Angaben im Freitextfeld)
- „Bitte die unterstützende Dokumentation hochladen“ Erläuterungen: „Bitte Daten hier ablegen oder hier klicken, um diese hochzuladen.““

- Nachdem der Hinweisgeber den Hinweis über die HWGS-Webseite abgegeben hat, kann dieser über die HWGS-Webseite die Informationen ergänzen, mit denen der/die Fallbearbeiter/in der Wilhelm Bötzel GmbH & Co. KG, einem Mitarbeiter/einer Mitarbeiterin der Wilhelm Bötzel GmbH & Co. KG, in einem Chat anonym kommunizieren und den Bearbeitungsstand einsehen kann. Hierfür muss der Hinweisgeber den Zugangscode in die HWGS-Webseite eingeben, der nach Abgabe des Hinweises dem Hinweisgeber auf der HWGS-Webseite angezeigt wird und die durch den Hinweisgeber gewählte 4-stellige PIN.

- Da ggf. die Anonymität gewahrt werden soll, ist ein Zurücksetzen des Zugangscode oder der PIN nicht möglich. Sollte der Hinweisgeber diese vergessen haben, ist ein neuer Hinweis anzulegen. Hierauf weist die HWGS-Webseite hin („Bitte legen Sie einen neuen Hinweis an, sollten Sie eines der beiden Elemente vergessen haben.“).

- Der Fallbearbeiter kann über die HWGS-Webseite für eventuelle Rückfragen mit dem Hinweisgeber kommunizieren.

- Daneben wird das HWGS als internes Dokumentationstool dienen, mit dem gemeldete Regelverstöße aus der Wilhelm Bötzel GmbH & Co. KG in einer zentralen Datenbank gespeichert und nachverfolgt werden. Dies betrifft zugleich sämtliche Kommunikationswege, auf denen Hinweise erfolgen können.

- Es werden keine personenbezogenen Kommunikationsdaten im Rahmen der Nutzung des HWGS gespeichert, sodass personenbezogene Daten nur verarbeitet werden, sofern der Beschwerdeführer diese auch im HWGS eingibt. Eine Verarbeitung personenbezogener Daten ist dann gegeben, wenn der Hinweisgeber entsprechende Angaben in den Freitextfeldern der Meldung vornimmt oder aber wenn er folgende Check-Box nach erfolgter Übermittlung des Hinweises anklickt: „Ich möchte über alle Fortschritte auf dem Laufenden gehalten werden.“

- Mit der Einrichtung des HWGS soll keine Meldepflicht der Mitarbeitenden der Wilhelm Bötzel GmbH & Co. KG begründet werden.

- Die Meldung soll einen Unternehmensbezug für die Wilhelm Bötzel GmbH & Co. KG vorweisen sowie einen Sachverhalt schildern, der eine schädigende Wirkung für beide Unter-

nehmen entfalten kann. Sachverhalte, die komplett außerhalb des Betriebs oder der betrieblichen Tätigkeit der beiden Unternehmen liegen, sollen nicht über das HWGS abgebildet werden, so zum Beispiel Straftaten von Mitarbeitenden ohne jeglichen Bezug zur betrieblichen Tätigkeit. Aufgrund der teilweise vorliegenden Freitextfelder ist dennoch eine Meldung ohne Unternehmensbezug möglich.

- Irrelevante Meldungen, die Sachverhalte betreffen, die außerhalb des Zwecks der HWGS liegen sollten, werden erst archiviert und dann gelöscht.

3. Beschreibung der Vorgänge, Art. 35 Abs. 7 lit. a) DS-GVO

Der Verarbeitungsvorgang (Erfassung, Speicherung, Veränderung, Übermittlung, Verknüpfung, Löschung) auf Basis der Beschreibung aus dem Verarbeitungsverzeichnis in seinen Grundzügen beschrieben.

3.1. Systematische Beschreibung der geplanten Verarbeitungsvorgänge

3.1.1. Rollen der Beteiligten

- Verantwortlicher der Datenverarbeitung ist die Wilhelm Bötzel GmbH & Co. KG, Wittener Straße 170 – 176, 58456 Witten, gesetzlich vertreten durch den Geschäftsführer Wilhelm Bötzel.
- Auftragsverarbeiter: Die Wilhelm Bötzel GmbH & Co. KG nutzt das Hinweisgebersystem der Aderhold Rechtsanwalts-gesellschaft mbH, Dortmund. Die Aderhold Rechtsanwalts-gesellschaft mbH hat mit der LegalTegrity GmbH, Platz der Einheit 2, 60323 Frankfurt am Main einen Vertrag über die Verarbeitung personenbezogener Daten abgeschlossen.
- Verarbeitungsvorgänge: Die Verarbeitungsvorgänge sind unter „2. Einleitung“ beschrieben. Zweck der Verarbeitung ist die Umsetzung der Verpflichtungen aus dem Hinweisgeberschutzgesetz. Die Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten findet sich in § 10 Hinweisgeberschutzgesetz. Da eine gesetzliche Vorgabe durch die Wilhelm Bötzel GmbH & Co. KG umgesetzt wird, bestehen die laut DS-GVO erforderlichen berechtigten Interessen.

3.1.1.1. Betroffene Personen(gruppen)

- Hinweisgeber
 - Kunden und Interessenten der Wilhelm Bötzel GmbH & Co. KG sowie deren Beschäftigte;
 - Lieferanten und Dienstleister der Wilhelm Bötzel GmbH & Co. KG sowie deren Beschäftigte;
 - Beschäftigte der Wilhelm Bötzel GmbH & Co. KG;
 - sonstige Hinweisgeber.
- Die durch einen Hinweis beschuldigten Personen

- Die im Hinweis sonstigen genannten Personen (Mitarbeitende oder sonstige Personen, etwa Geschäftspartner, Amtsträger etc., z. B. in ihrer Funktion als Zeugen)
- Verarbeitung der personenbezogenen Daten der Nutzer (etwa Administratoren sowie sonstige zur Fallbearbeitung berechnigte Personen)

3.1.1.2. Besonders gefährdete Personen(gruppen)

Als besonders gefährdete Personen können minderjährige Mitarbeitende der Wilhelm Bötzel GmbH & Co. KG (bspw. minderjährige Auszubildende u.a. im Rahmen der Abwesenheitsplanung für die Berufsschule) von der Verarbeitung personenbezogener Daten betroffen sein. Die besondere Schutzbedürftigkeit dieser Personen kennt die DS-GVO z.B. in den Erwägungsgründen 38, 58, 65, 71 und 75 sowie Art. 6 Abs. 1 lit. f) letzter Hs., Art. 8 ,12 Abs. 1 Hs. 2, Art. 57 Abs. 1 lit. b) DS-GVO an.

Je nach Inhalt der Meldung ist nicht auszuschließen, dass auch Daten von Opfern von Straftaten verarbeitet werden, z. B. wenn die Meldung über Körperverletzungen, Belästigungen, Beleidigungen berichtet.

3.1.2. Art

- Speicherung von Informationen über ein mögliches Fehlverhalten, die ein Hinweisgeber abgegeben hat. Der Hinweisgeber soll nur auf freiwilliger Basis seine personenbezogenen Daten angeben. Wenn eine Angabe erfolgt, soll er eine Einwilligung im Tool abgegeben, die dort dokumentiert wird. Der jeweilige Fallbearbeiter kann sich über eine Zwei-Faktor-Authentifizierung in die HWGS-Webseite einloggen und auf die jeweiligen Daten zugreifen. Dabei ist der Kreis der Zugriffsberechnigten auf einen Personenkreis von drei Personen in der Paketvariante Professional beschränkt.
- Eine Übermittlung der Daten bspw. an die Strafverfolgungsbehörden ist dann denkbar, wenn der Hinweisgeber Indizien für ein strafbares Verhalten mitteilt.

3.1.3. Umfang

- Die Datenmengen sind meist sehr gering, weil nur eine Beschreibung von Beobachtungen erfolgt und hierbei wenige personenbezogene Daten übermittelt werden. Die Beobachtungen können strafbare Handlungen betreffen, die beobachtet worden sind oder von denen die hinweisgebende Person gehört hat.
- Erfasst werden meist nur personenbezogene Daten desjenigen, dem ein Fehlverhalten vorgeworfen wird, möglicher Zeugen bzw. Beobachter und in Ausnahmefällen die der hinweisgebenden Person.

3.1.4. Dauer

Bearbeitung eines Hinweises – Prozessphasen:

Aktion	Prozessphase	Dauer
Neuer Hinweis	Ausstehend	--
Eingangsbestätigung	In Arbeit Untersuchung des Vorfalls Rückfragen an Hinweisgeber	1 Woche
Ergebnis kommunizieren	Review Feedback des Hinweisgebers	3 Monate
Bearbeitung abschließen	Geschlossen	Flexibel
Archivieren	Archiviert	3 Jahre
Automatische Löschung aller Daten	Gelöscht	3 Jahre nach Abschluss des Verfahrens; längere Speicherung bei berechtigtem Interesse im Einzelfall möglich. Im Rahmen einer Einzelfallprüfung erfolgt eine Orientierung an den zivil- und strafrechtlichen Verjährungsfristen wie es für die Zwecke der Untersuchung und der anschließenden Durchführung von zivil- oder strafrechtlichen Maßnahmen gegen die Beteiligten erforderlich ist..

3.1.5. Orte

- Alle Informationen, die in der Datenbank der HWGS von der Wilhelm Bötzel GmbH & Co. KG gespeichert werden, werden von einem Subunternehmer (Telekom Deutschland GmbH, Landgraben 151, 53227 Bonn) innerhalb des EWR (Europäischer Wirtschaftsraum) gehostet, nämlich in Deutschland.

3.1.6. Mittel/eingesetzte Technik

- Der Subunternehmer Telekom Deutschland GmbH hostet die die Datenbank in der Open Telekom Cloud, die in zwei redundanten Rechenzentren in Magdeburg und Biere (EWR) betrieben werden.

3.1.7. Betroffene Datenkategorien

- Ggf. Name, Adresse, E-Mail-Adresse, Telefonnummer der Beschuldigten, der Zeugen, weiterer Beteiligter und der hinweisgebenden Person (wenn sich diese dazu entschließt, nicht anonym zu melden). Darüber hinaus stehen diverse Freitextfelder und die Möglichkeit zum Anhängen von Beweisunterlagen zur Verfügung, in denen zum Tathergang berichtet wird. Diese Informationen können Angaben u. a. zu dem Aufenthaltsort oder zu geführten Telefonaten, versendeten E-Mails enthalten.
- Je nach Inhalt der Meldung ist nicht auszuschließen, dass auch Daten von Opfern verarbeitet werden, z. B. wenn in Meldungen über Körperverletzung, Belästigung, Beleidigungen oder ähnliches berichtet werden.

3.1.8. Weitergabe

- Geplant? Ja.
- An wen und zu welchem Zweck?
 - Externe Kanzlei Aderhold Rechtsanwalts-gesellschaft mbH: Zwecks etwaiger Begleitung, weitergehender Untersuchung und Lösungsfindung.
 - An den Auftragsverarbeiter LegalTegrity GmbH als Unter-Vertragspartner der Aderhold Rechtsanwalts-gesellschaft mbH: Zur Durchführung der Auftragsverarbeitung
 - Strafverfolgungsbehörden oder Aufsichtsbehörden auf Anforderung.

3.1.9. Zugriff auf die Daten

- Das Rollen- und Berechtigungskonzept zum HWGS setzt den zweckgebundenen Umfang und Rahmen der Datenverarbeitung auf die folgenden Rollen fest: Administrator, Support-Rolle, General Case Manager, General Case Reader und Nutzer.
- Die Zugriffs- und Verarbeitungsrechte ergeben sich je aus der folgenden Übersicht:

Berechtigungen	Admin	Support-Rolle	General Case Manager	General Case Reader	Nutzer
Einstellungen <ul style="list-style-type: none"> - Organisationseinstellungen und –status bearbeiten - Benutzerkonten anlegen, bearbeiten und Rollen festlegen - Up-/Downgrade Paket (inkl. zusätzlicher Benutzerkonten und Sprachen) - Zahlungsdetails bearbeiten 	■	■			
Dashboard: Daten zum Hinweisaufkommen und der Bearbeitung einsehen	■	■	■	■	■
Lese- und Bearbeitungsberechtigungen für Hinweise vergeben	■		■		
Alle Hinweise einer Organisation bearbeiten	■		■		
Alle Hinweise einer Organisation lesen	■		■	■	

Zugeordnete Hinweise lesen und bearbeiten					Als: Case Manager
Zugeordnete Hinweise lesen					Als: Case Reader

- Dabei sind die Rollen wie folgt festgelegt:

Organisation	Funktion	Name	Berechtigung
Aderhold Rechtsanwaltsgesellschaft mbH	Rechtsanwalt/Partner	Dr. Christian H. Müller	Administrator
Wilhelm Bötzel GmbH & Co. KG	Qualitätsmanagement	Angela Perkun	General Case Manager
Wilhelm Bötzel GmbH & Co. KG		Kai-Uwe Becker	General Case Manager
--	n.n.	Wechselnd bei Bedarf	Case Manager
--		Wechselnd bei Bedarf	Case Reader

- Weitere Nutzer können bei Bedarf gegen Gebühr hinzugefügt werden. Um den Nutzerkreis möglichst klein zu halten, soll von dieser Möglichkeit kein Gebrauch gemacht werden.

3.1.10. Eingehende Hinweise können intern allein der mit den Aufgaben der internen Meldestelle gem. § 15 HinSchG beauftragte Mitarbeiter der Wilhelm Bötzel GmbH & Co. KG und der zuständige Berufsträger der Aderhold Rechtsanwaltsgesellschaft mbH lesen.

3.1.11. Prüfung der geplanten Aufbewahrungsfrist

- Prüfung, ob die Daten wirklich erforderlich sind (vgl. auch Art. 5 Abs. 1 lit. c) DS-GVO). Die Verarbeitung der angegebenen Daten ist zur Zweckerreichung erforderlich.
- Prüfung, wie transparent die Bearbeitung gegenüber Betroffenen erfolgt.

3.2. Zwecke der Datenverarbeitung

Das HWGS dient der Prävention und Aufklärung rechtswidrigen und / oder geschäftsschädigenden Verhaltens durch Mitarbeitende der Wilhelm Bötzel GmbH & Co. KG oder sonstige Personen, sofern ein Unternehmensbezug vorliegt.

Die Wilhelm Bötzel GmbH & Co. KG führt das HWGS ein, um damit dem Gesetz für einen besseren Schutz hinweisgebender Personen (vom 31. Mai 2023 (BGBl. 2023 I Nr. 140)) zu entsprechen. Diese Richtlinie sieht für Unternehmen einer bestimmten Größe die Implementierung eines Hinweisgebersystems zwingend vor.

3.3. Stand der Technik in diesem Bereich/ Innovationsqualität

Hinweisgebersysteme kommen in manchen Sektoren bereits seit längerer Zeit zum Einsatz (vgl. etwa § 25a Abs. 1 S. 6 Nr. 3 KWG in der Fassung vom 1. Januar 2014). Jedenfalls seit Verabschiedung der sog. EU-Whistleblower-Richtlinie (EU) 2019/1937 und der damit einhergehenden Umsetzungspflicht für die Mitgliedsstaaten bis zum 17. Dezember 2021 nach Art. 26 Abs. 1 der Richtlinie besteht auch sektorübergreifend Handlungsbedarf. Mit dem deutschen Hinweisgeberschutzgesetz sind die entsprechenden Anforderungen in nationales Recht umgesetzt worden und unmittelbar anwendbar. Hinweisgebersysteme, wie das zuvor beschriebene HWGS der Aderhold Rechtsanwalts-gesellschaft mbH, werden dabei von verschiedenen Anbietern am Markt angeboten und es handelt sich hierbei um eine moderne, aber nicht absolut innovative Art und Weise der Datenverarbeitung.

3.4. Rechtsgrundlagen / ggf. Berechtigte Interessen

Datenverarbeitung	Rechtsgrundlage	Erläuterung
Verarbeitungen im Rahmen einer ersten Speicherung eines Hinweises („Entgegennahme eines Hinweises“)	Art. 6 Abs. 1 lit. c) DS-GVO i.V.m. der deutschen Umsetzungsvorschrift von Art. 8 Abs. 1 DS-GVO der Hinweisgeber-RL	Sofern die Wilhelm Bötzel GmbH & Co. KG einer gesetzlichen Pflicht zur Datenverarbeitung unterliegt, sind die entsprechenden Datenverarbeitungen nach Art. 6 Abs. 1 lit. c) DS-GVO i.V.m. der gesetzlichen Pflicht gerechtfertigt.
	Art. 6 Abs. 1 lit. f) DS-GVO	Die Wilhelm Bötzel GmbH & Co. KG hat ein legitimes und überwiegendes Interesse an der Entgegennahme von Hinweisen, die geeignet sind, eine präventive Verhinderung oder repressive Aufklärung von Verstößen zu ermöglichen.
Verarbeitung im Rahmen von Folgemaßnahmen („Prüfung eines Hinweises“)	Art. 6 Abs. 1 lit. c) DS-GVO	Sofern sich die Hinweise auf die Aufdeckung von Straftaten von Beschäftigten beziehen, soweit konkrete Anhaltspunkte den Verdacht begründen, dass der Beschäftigte eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind, ist die Verarbeitung gerechtfertigt. <u>Interessenabwägung:</u> Im Rahmen der Interessenabwägung ist zu berücksichtigen, dass die betroffenen Mitarbeiter um die Verarbeitung ihrer Daten wissen, insbesondere durch eine detaillierte Datenschutzerklärung und Mitteilungen im Intranet. Die

Datenverarbeitung	Rechtsgrundlage	Erläuterung
		<p>Sicherheit ihrer Daten ist überdies durch technische und organisatorische Sicherungsmaßnahmen gewährleistet.</p> <p>Insbesondere werden die Daten nur streng zweckgebunden verarbeitet und nach Abschluss der Ermittlungen in datenschutzkonformer Weise gelöscht. Die Gefahr einer Stigmatisierung oder Viktimisierung von Mitarbeitern wird auf diese Weise minimiert.</p> <p>Zugleich wird durch eindeutige Anweisungen sichergestellt, dass das Hinweisgebersystem nicht zur Aufklärung von lediglich geringfügigen Verstößen missbraucht wird. Die Datenverarbeitungen werden daher durch die Wilhelm Bötzel GmbH & Co. KG nur aktiv durchgeführt, wenn das Aufklärungsinteresse von beiden Unternehmen durch eine behauptete Straftat oder einen ernsten Regelverstoß sehr hoch ist. Auch dies führt dazu, dass das berechnete Interesse von beiden Unternehmen gegenüber den Rechten der betroffenen Personen überwiegt.</p>

3.5. Speicherfrist

Datenkategorie	Speicherfrist	Rechtsgrundlage bei fort-dauernder Speicherung
Hinweise, einschließlich solcher mit personenbezogenen Daten, über die interne Meldestelle	Die Dokumentation wird drei Jahre nach Abschluss des Verfahrens gelöscht. Die Dokumentation kann länger aufbewahrt werden, um die Anforderungen nach diesem Gesetz oder nach anderen Rechtsvorschriften zu erfüllen, solange dies erforderlich und verhältnismäßig ist.	§ 11 Abs. 3 HinSchG

3.6. Einhalten datenschutzrechtlicher Kernanforderungen

Szenario	Anforderung	Antwort	Begründung/Erläuterung
Jedwede Verarbeitung personenbezogener Daten	Ist sichergestellt, dass die verarbeiteten Daten faktisch korrekt sind?	Ja	Daten werden regelmäßig durch Interaktionen mit dem Hinweisgeber und sonstigen Personen erneuert und aktualisiert. Nicht mehr zutreffende Daten werden dadurch regelmäßig ersetzt.
	Ist sichergestellt, dass die betroffenen Personen über die sie betreffenden Datenverarbeitungen informiert werden?	Ja	Die Betroffenen können auf die allgemein zugänglichen Datenschutzhinweise, die alle notwendigen Informationen zu den Datenverarbeitungen beinhalten, zugreifen. In anderen Fällen ist nach § 29 Abs. 1 S. 1 BDSG eine Information nicht erforderlich.
	Ist sichergestellt, dass betroffene Personen ihre datenschutzbezogenen Rechte ausüben können?	Ja	Die Verantwortung zur Beantwortung von Betroffenenanfragen liegt bei der gem. § 15 HinSchG beauftragten Person, aktuell Frau A. Perkun und Herr K-U. Becker als Mitarbeiter/-in der Wilhelm Bötzel GmbH & Co. KG.
Drittlandtransfers	Werden Daten aus dem EWR in einen Staat außerhalb des EWR übermittelt?	Nein	
	Falls die obige Frage bejaht, wurde: Ist die Datenübermittlung durch ein rechtliches Instrumentarium für Drittlandtransfers abgesichert?	N/A	
Änderung von Verarbeitungszwecken	Werden Daten, die ursprünglich für einen bestimmten Zweck erhoben wurden, nunmehr für einen anderen (oder ausgeweiteten) Zweck verarbeitet?	Nein	
	Falls eine Zweckänderung bejaht, wurde: Ist der neue Verarbeitungszweck mit dem alten Verarbeitungszweck „vereinbar“?	N/A	
Einschalten weisungsgebundener Dienstleister	Falls für die hier relevanten Datenverarbeitungen weisungsabhängige	Ja	Der eingesetzte Dienstleister LegalTegrity GmbH ist ein bekannter Dienstleister, von dessen Zuverlässigkeit

	Dienstleister eingebunden werden: Wurden diese sorgfältig ausgewählt und falls ja, auf welche Weise?		ausgegangen werden kann. Konkrete Anhaltspunkte, dass eine Ausnahme besteht, liegen nicht vor.
	Wurde mit dem Auftragsverarbeiter ein Vertrag über die Auftragsverarbeitung geschlossen?	Ja	Die Aderhold Rechtsanwaltsgesellschaft mbH hat mit der LegalTegrity GmbH einen Vertrag über die Verarbeitung personenbezogener Daten abgeschlossen.

3.7. Genehmigte Verhaltensregeln und Zertifizierungen

n/a

4. Bewertung der Notwendigkeit und Verhältnismäßigkeit, Art. 35 Abs. 7 lit. b) DS-GVO

Die Verarbeitungstätigkeit ist in ihrer konkreten Ausprägung für die genannten Zwecke notwendig und verhältnismäßig. Insbesondere lässt sich der Zweck nicht mit mildereren Mitteln erreichen und die Datenverarbeitung erfolgt unter Einsatz von im Folgenden näher beschriebenen Datensicherheitsmaßnahmen.

4.1. Speicherung des Hinweises und Ermittlungen durch die Wilhelm Bötzel GmbH & Co. KG unter Nutzung des Hinweisgebersystems der Aderhold Rechtsanwaltsgesellschaft mbH

Die Wilhelm Bötzel GmbH & Co. KG verarbeitet die Hinweise einschließlich weniger Daten über die Umstände des Hinweises (ggf. den Namen des Hinweisgebers, falls dieser freiwillig genannt wird). Die Hinweise werden gespeichert und im Anschluss insofern genutzt, als dass die zuständigen Fallbearbeiter sie verwenden, um die Ermittlungen durchzuführen.

Ohne die Speicherung und die Nutzung des Hinweises einschließlich der möglichen Kommunikation mit dem Hinweisgeber ist es im Regelfall unmöglich, den Sachverhalt aufzuklären. Die Daten werden nur zur Aufklärung des Fehlverhaltens und zur Ergreifung rechtmäßiger Maßnahmen zur Sanktionierung und zur Vorbeugung genutzt. Insofern sind die Datenverarbeitungen geeignet, den Zweck zu erreichen. Ein milderer gleichwirksames Mittel ist nicht ersichtlich.

Die Speicherung und Nutzung ist auch angemessen entsprechend dem in Art. 5 Abs. 1 lit. c DS-GVO verankerten Grundsatz der Datenminimierung.

Insbesondere sind – auch in Übereinstimmung mit den Empfehlungen der Datenschutzkonferenz, Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines vom 14. November 2018 – folgende für die Einhaltung der Verhältnismäßigkeit relevante Aspekte gewährleistet:

- Der Kreis der zugangsberechtigten Personen sollte eng definiert werden. Dies ist bei der Wilhelm Bötzel GmbH & Co. KG der Fall. Lediglich mit der Investigation unmittelbar befasste Fallbearbeiter können nach erfolgter Zwei-Faktor-Authentisierung die Daten einsehen.
- Darüber hinaus sollte definiert werden, welches Fehlverhalten (und ggfs. welche Personengruppen) Gegenstand des Hinweisgebersystems sein sollen. Auf das ist gegeben. Sowohl Datenschutzhinweise als auch ein entsprechender Eintrag im Intranet stellen klar, dass das HWGS nicht für die Meldung „weicher“ Verstöße im Sinne etwa lediglich als unangemessen empfundenen Verhaltens genutzt werden sollte.
- Die Richtigkeit der mitgeteilten Informationen sollte überprüft werden. Hierzu dient gerade die Aufnahme von Ermittlungen.
- Es sollten Fristen zur Datenlöschung definiert und eingehalten werden. Dies ist insofern gewährleistet, als Daten bei abgeschlossener Ermittlung, die nicht zu weiterführenden rechtlichen Schritten führen, innerhalb der von HinSchG definierten Fristen nach Abschluss der Ermittlungen gelöscht werden.

4.2. Weitergabe der Daten an den Auftragsverarbeiter

Die Weitergabe der Daten an die Aderhold Rechtsanwaltsgesellschaft mbH als frei entscheidender Berater und die LégalTegrity GmbH ist nicht zwingend notwendig, um ein Hinweisgebersystem zu betreiben. Hierdurch wird jedoch die Integrität und Vertraulichkeit der personenbezogenen Daten weitaus besser gewährleistet als ohne die Zwischenschaltung eines derartigen Dienstleisters.

Im Sinne einer verhältnismäßigen Lösung ist dies eine sachgerechte Vorgehensweise, die sich zugleich am oberen Marktstandard orientiert. Die Weitergabe der Daten an ein externes Unternehmen und das mit dieser Weitergabe verbundene erhöhte Risiko für die Rechte und Freiheiten der betroffenen Personen steht keineswegs außer Verhältnis zum Zweck der Aufklärung potenziellen Fehlverhaltens. Ganz im Gegenteil wird dieses zusätzlich geschaffene Risiko gleichsam überkompensiert durch die damit geschaffene optimierte Möglichkeit, den Sachverhalt aufzuklären und gleichzeitig den Schutz der personenbezogenen Daten zu gewährleisten. Im Übrigen ist auch durch den Abschluss eines den Anforderungen des Art. 28 Abs. 3 DS-GVO genügenden Auftragsverarbeitungsvertrages betreffend die Durchführung von Untervertragsdienstleistungen eine Kompensation des Risikos gewährleistet.

Eine alternative Vorgehensweise, die ohne Zwischenschaltung eines sorgfältig ausgewählten Dienstleisters die Vertraulichkeit der Daten gleichermaßen gewährleistet, ist nicht denkbar. Wenn die Wilhelm Bötzel GmbH & Co. KG selbst diese Daten speichert, ist das Risiko einer unbeabsichtigten Offenlegung der Identität innerhalb der Wilhelm Bötzel GmbH & Co. KG höher als bei der Einschaltung eines auf das Datengeheimnis verpflichteten, spezialisierten Dritten.

4.3. Übermittlung an Behörden

Auch die Übermittlung an Behörden erfolgt lediglich in notwendigen Fällen, nämlich wenn das einschlägige nationale Recht (insb. Strafrecht) diese Übermittlung erfordert oder zumindest zulässt. In diesem Fall liegt der Verarbeitungszweck ebenfalls in der Aufklärung des Fehlverhaltens, aufgrund

der besonderen Schwere der in Rede stehenden Handlungen jedoch nicht lediglich durch die Wilhelm Bötzel GmbH & Co. KG selbst, sondern durch staatliche Stellen.

Hierzu erfolgt die Datenübermittlung nur insoweit, wie die Informationen zur Aufklärung des Sachverhalts beitragen können. Dadurch wird die Verhältnismäßigkeit der Datenverarbeitungen gewährleistet.

5. Risikobewertung, Art. 35 Abs. 7 lit. c) DS-GVO

Die nachfolgend dokumentierte Risikobewertung identifiziert die Risiken für die Rechte und Freiheiten der betroffenen Personen (Risikoidentifikation) und unterzieht diese einer Analyse (Risikoanalyse). Im Einzelnen wurden die folgenden Risiken bewertet:

- Verlust der Vertraulichkeit (z. B. unbefugter Zugriff auf personenbezogene Daten)
- Verlust der Integrität (z. B. unerwünschte Änderung von personenbezogenen Daten)
- Verlust der Verfügbarkeit (Belastbarkeit) (z. B. Verlust von personenbezogenen Daten)

Daraus ergeben sich die folgenden Risikowerte, die anhand Eintrittswahrscheinlichkeit einer Bedrohung sowie den zu erwartenden Auswirkungen gebildet werden.

Sowohl die Schwere des möglichen Schadens als auch die Wahrscheinlichkeit des Eintritts des Risikos, die mit den beabsichtigten Datenverarbeitungen einhergehen, werden im Folgenden anhand einer viergliedrigen Skala beurteilt:

Schwere des möglichen Schadens / Einschätzung der Schadensauswirkungen (physisch, materiell und immateriell)

Gering	Die Betroffenen sind entweder nicht betroffen oder werden auf kleinere Unannehmlichkeiten stoßen, die sie problemlos überstehen/aushalten können
Mittel	Die betroffenen Personen können auf erhebliche Unannehmlichkeiten stoßen, die sie trotz geringer Schwierigkeiten überwinden können.
Hoch	Die betroffenen Personen können erhebliche Konsequenzen erleiden, die sie nur mit echten und ernststen Schwierigkeiten überwinden können.
Sehr hoch	Die Betroffenen können auf signifikante oder gar irreversible Konsequenzen stoßen, die sie nicht überwinden können.

Bemessung der Eintrittswahrscheinlichkeit

Unwahrscheinlich	Für die ausgewählte Risikoquelle scheint es nicht sehr wahrscheinlich zu sein, eine Schwachstelle eines unterstützenden Wertes auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Papierdokumenten aus einem Raum, der durch ein Ausweislesegerät und einen Zugangscode gesichert ist).
Möglich	Für die ausgewählte Risikoquelle scheint es schwierig zu sein, eine Schwachstelle eines unterstützenden Wertes auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Papierdokumenten aus einem Raum, der durch ein Ausweislesegerät gesichert ist).
Wahrscheinlich	Für die ausgewählte Risikoquelle scheint es möglich zu sein, eine Schwachstelle eines unterstützenden Werts auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Papierdokumenten aus einem Büro, welches nur zugänglich ist, nachdem man einen Empfang passiert hat).
Sehr wahrscheinlich	Für die ausgewählte Risikoquelle scheint es einfach zu sein, eine Schwachstelle eines unterstützenden Wertes auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Papierdokumenten aus einer öffentlich zugänglichen Lobby).

6. Bisher geplante / bestehende Abhilfemaßnahmen

6.1. Typ der Risikobehandlung

Es existieren vier verschiedene Möglichkeiten, mit Risiken zu verfahren, wobei selbstverständlich nicht immer jede Möglichkeit im Einzelfall zur Verfügung steht:

6.1.1. Risikominimierung durch das Ergreifen von Maßnahmen:

Die DS-GVO stellt in Art. 32 Abs. 1 Option der Risikominderung durch das Ergreifen von (Datenschutz-) Maßnahmen dar und verlangt, dass mindestens die Umsetzung der folgenden Maßnahmen geprüft werden soll:

- Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
- Sofern Risiken durch die Einleitung von Maßnahmen verringert werden sollen, sollte eine entsprechende Maßnahmenliste geführt werden, die dokumentiert, welche Maßnahme geplant ist, wer für die Umsetzung verantwortlich ist, und wie die zeitliche Planung sich darstellt, die Umsetzung abzuschließen.

6.1.2. Risikovermeidung:

Die Verarbeitungstätigkeit wird so verändert, dass eine Gefährdung der Betroffenen ausgeschlossen ist. Dies kann erfolgen durch:

- Veränderungen der Abläufe innerhalb der Verarbeitungstätigkeit;
- Veränderungen der Rahmenbedingungen außerhalb der Verarbeitungstätigkeit;
- Verzicht auf die Verarbeitung einzelner, typischerweise besonders sensibler Datenkategorien;
- Einstellung der Verarbeitungstätigkeit.

6.1.3. Risikotransfer auf Dritte:

Der Transfer verlagert Risiken auf Dritte. Zumindest verschiedene finanzielle Risiken lassen sich beispielsweise durch den Abschluss einer Versicherung abfedern. Auch wenn der Risikotransfer eine Standardrisiko-Strategie etwa nach IT-Grundschutz ist, ist er im Bereich des Datenschutzrechts häufig wenig geboten. Denn der Risikotransfer mag evtl. finanzielle Schäden abmildern, jedoch nicht alle Risiken beseitigen. Denn etwa bleibt der Verantwortliche bei der Einschaltung eines Dienstleisters (Art. 28 DS-GVO) oder weiteren Verantwortlichen (Art. 26 DS-GVO) (mit-)verantwortlich, auch schützt ein Risikotransfer nur eingeschränkt gegen Ansehensverluste oder juristische Konsequenzen.

6.1.4. Risikoakzeptanz:

Risikoakzeptanz ist die bewusste Entscheidung, keine weiteren Maßnahmen zu treffen, insbesondere sofern vorbeschriebene Maßnahmen nicht möglich waren oder ökonomisch als nicht vertretbar erachtet wurden. Insbesondere bei geringen Risiken bietet sich dann an, diese schlicht hinzunehmen; das umfasst insbesondere solche Risiken, bei denen der mögliche Schaden oder die Eintrittswahrscheinlichkeit niedrig sind.

Zu beachten ist, dass die Risikoakzeptanz zwar eine valide Risikostrategie an dieser Stelle ist, die DSFA aber insgesamt deshalb möglicherweise zum unerwünschten Ergebnis gelangt, dass etwa eine behördliche Vorabprüfung („Vorherige Konsultation“ nach Art. 36 DS-GVO) erforderlich werden kann. Auch sollte insbesondere diese Risikostrategie mit der obersten Leitung abgestimmt sein bzw. bestätigt werden.

Die Wilhelm Bötzel GmbH & Co. KG entscheidet sich für den Ansatz der Risikominimierung.

6.2. Beschreibung der Gründe für die Auswahl des Risikobehandlungstyps

Die Entscheidung für den Ansatz der Risikominimierung beruht darauf, dass eine Verarbeitung der vorgenannten personenbezogenen Daten notwendig ist, um die zuvor beschriebenen Verarbeitungszwecke zu verfolgen. Der Ansatz der Risikovermeidung kann daher nicht verfolgt werden, ebenso wie die – aufgrund der Stellung der Betroffenen teilweise als Arbeitnehmer – nicht vertretbaren Folgen der Ansätze des Risikotransfers auf Dritte sowie der Risikoakzeptanz.

6.3. Dokumentation der Maßnahmen

- Es gibt ein restriktives Berechtigungsmanagement mit nur drei Berechtigten;
- Zwei-Faktor-Authentisierung der Fallbearbeiter, um auf die personenbezogenen Daten zuzugreifen;
- Schutz des Zugriffs auf die Meldung mittels einer nur dem Meldenden bekannten selbst vergebenen 4-stelligen PIN sowie der Eingabe des Zugangscodes (letztere wird nur dem Hinweisgeber angezeigt, nachdem dieser die Meldung getätigt hat);

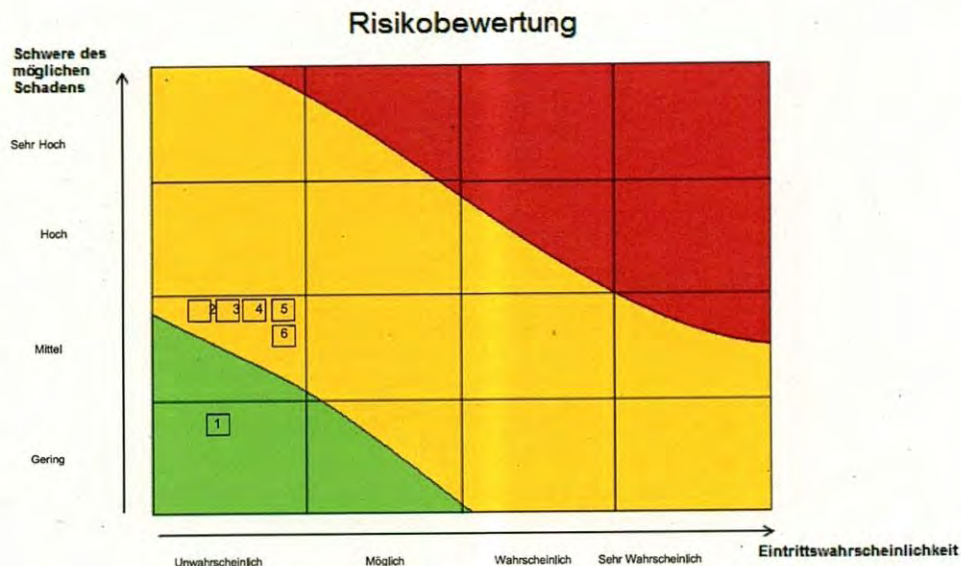
6.4. Zusammenfassung Risikoanalyse

	Thema	Mögliches Schadensereignis	Schwere des möglichen Schadens	Eintrittswahrscheinlichkeit	Erläuterung	Abhilfemaßnahmen	Schwere des möglichen Schadens ...	Eintrittswahrscheinlichkeit ...
1	Verarbeitung ohne/gegen den Willen des Hinweisgeber	Speicherung der Identität des Hinweisgebers ohne Zustimmung	Hoch	Unwahrscheinlich	Die Speicherung der Identität könnte zu hohen immateriellen Schäden führen. Ohne geeignete Abhilfemaßnahmen könnte dies häufig vorkommen	Die Identität des Hinweisgebers wird lediglich gespeichert, wenn dieser seine Identität freiwillig offenbart hat. Die Datenschutzerklärung weist ebenso wie weitere Nutzungshinweise ausdrücklich auf die Möglichkeit hin, den Hinweis anonym zu erteilen. Gleichzeitig soll auch bewusst die Möglichkeit angeboten werden, den Hinweis mit Personenbezug zu erteilen. Dadurch können nicht nur Hinweise mitunter besser nachvollzogen werden, sondern es	... nach Abhilfemaßnahme	Unwahrscheinlich

	Thema	Mögliches Schadensereignis	Schwere des möglichen Schadens	Eintrittswahrscheinlichkeit	Erläuterung	Abhilfemaßnahmen	Schwere des möglichen Schadens ...	Eintrittswahrscheinlichkeit ...
2	Datennutzung im Zuge der Durchführung von Ermittlungen	Persönlichkeitsrechtsverletzung, etwa durch (versehentliche) Offenbarung von unsubstantiierten Verdächtigungen	Hoch	Unwahrscheinlich	Eine mögliche Rufschädigung könnte je nach des in Rede stehenden Fehlverhaltens einen erheblichen Schaden bei der jeweiligen betroffenen Person bedeuten.	Beachtung sämtlicher Sicherheitsstandards in organisatorischer und technischer Hinsicht, u.a. mit strengen Zugriffsberechtigungen.	Mittel	Unwahrscheinlich
3	Unzulässige Bearbeitung von Betroffenenanfragen		Hoch	Unwahrscheinlich	Eine unzulässige Auskunft etwa könnte den Hinweisgeber umfangreichen Sanktionen aussetzen, aber auch für Rufschädigung sorgen. Eine unzulässige Löschung	Implementierung einer vordefinierten Vorgehensweise hinsichtlich des Umgangs mit Betroffenenanfragen, insb. mit Anträgen zur Auskunft, Korrektur und Löschung von Daten;	Mittel	Unwahrscheinlich

	Thema	Mögliches Schadensereignis	Schwere des möglichen Schadens	Eintrittswahrscheinlichkeit	Erläuterung	Abhilfemaßnahmen	Schwere des möglichen Schadens ...	Eintrittswahrscheinlichkeit ...
					<p>oder Korrektur könnte Beweise vernichten. Ohne klare Prozesse besteht eine substanzielle Wahrscheinlichkeit, derartige Anfragen in unzulässiger Weise zu bearbeiten.</p>	<p>aktuell ist dies mit den „[●]“ bereits existent.</p>		
4	Verstoß gegen Datenrichtigkeit	Speicherung inkorrekturer Daten bei fehlerhaftem Inhalt des gespeicherten Hinweises	Hoch	Unwahrscheinlich		<p>Unmittelbar nach Eingang des Hinweises wird durch erfahrene Mitarbeiter überprüft, ob die Anschulldigungen einen substantiierten und schlüssigen Kern aufweisen. Im Anschluss werden die Ermittlungen effizient durchgeführt. Sobald die Fehlerhaftigkeit von Informationen bemerkt wird, werden diese Daten korrigiert. Daten, die nicht zu weiterführenden rechtlichen Schritten führen, werden gelöscht. Dadurch</p>	Mittel	Unwahrscheinlich

	Thema	Mögliches Schadensereignis	Schwere des möglichen Schadens	Eintrittswahrscheinlichkeit	Erläuterung	Abhilfemaßnahmen	Schwere des möglichen Schadens ...	Eintrittswahrscheinlichkeit ...
5	Offenlegen Allgemeine Daten	Möglichkeit der ungewollten Veröffentlichung personenbezogener Daten	Hoch	Unwahrscheinlich	Risiko der Stigmatisierung und Viktimisierung des Hinweisgebers oder des Betroffenen.	Einsatz der dargelegten TOM.	Mittel	Unwahrscheinlich
6	Löschung von Daten	Datenschutzverletzung durch fortdauernde Speicherung von Daten trotz Zweckfortfalls	Hoch	Unwahrscheinlich	Die Speicherung würde ohne Lösroutine oftmals über den Zeitpunkt des Zweckfortfalls hinausgehen. Die reine fortdauernde Speicherung würde einen eher geringen Schaden bedeuten; hier- mit verbunden ist jedoch ein fortdauerndes Risiko der unbefugten Offenlegung.	Durch strikte Löschrfristen mit präziser Festlegung von Aufbewahrungs- und Löschrfristen für verschiedene Szenarien ist dieses Risiko minimiert.	Mittel	Unwahrscheinlich



6.5. Folgerungen aus der Risikobewertung

Die kritischsten Datenverarbeitungen sind in (1) der Speicherung falscher Daten, (2) der Offenbarung von falschen oder unsubstantiierten Verdächtigungen, (3) der fehlerhaften Bearbeitung von Betroffenenanfragen (etwa eines Auskunfts- oder Löschbegehrens des Beschuldigten) und der (4) Möglichkeit der ungewollten Veröffentlichung von Daten, oder unbefugter Zugriff darauf zu sehen.

Ersteres ist einem Hinweisgebersystem immanent, da der Verantwortliche nicht absolut zuverlässig verhindern kann, dass falsche Informationen gespeichert werden. Die potenziellen hinweisgebenden Personen werden darüber aufgeklärt, dass bewusste Fehlbehauptungen arbeits-, zivil- und strafrechtliche Konsequenzen nach sich ziehen können. Gerade im Schutze der Anonymität kann nicht ausgeschlossen werden, dass womöglich – auch unbeabsichtigt – falsche Informationen gespeichert werden können.

Die Wilhelm Bötzel GmbH & Co. KG begegnet diesem Risiko durch eine bestmögliche Aufklärung des Sachverhaltes und konsequentem Verhindern der Offenlegung der Informationen, wenn die Ermittlungen noch nicht abgeschlossen sind und/oder die Behauptungen sich nicht als nachweislich wahr und pflichtwidrig erwiesen haben.

Der versehentlichen Offenbarung falscher oder unsubstantiiertes Verdächtigungen sowie der Möglichkeit der ungewollten Veröffentlichung von Daten, oder des unbefugten Zugriffs darauf wird durch die konsequente Beachtung sämtlicher Sicherheitsstandards in organisatorischer und technischer Hinsicht begegnet. Dies umfasst u.a. strenge Zugriffsberechtigungen, aber auch eine schnellstmögliche Löschung der Daten und andere Maßnahmen wie die Einbindung eines erfahrenen und hochspezialisierten Dienstleisters.

Den Risiken wird mit den vorhandenen Sicherheitsmaßnahmen in sachgerechter Weise begegnet. Sie stehen nicht außer Verhältnis zu den Verarbeitungszwecken. Wir sehen keine Restrisiken, die durch die beschriebenen Maßnahmen nicht hinreichend eingedämmt wären, so dass die geplante Verarbeitung im Ergebnis im Einklang mit der DS-GVO steht, wenn die Abhilfemaßnahmen wie beschrieben umgesetzt sind.

7. Relevante Stellungnahmen

7.1. Rat des Datenschutzbeauftragten

Bei der Durchführung einer Datenschutz-Folgeabschätzung ist der Rat des Datenschutzbeauftragten einzuholen, Art. 35 Abs. 2 DS-GVO.

Der Datenschutzbeauftragte hat keine Bedenken gegen die Form der Datenverarbeitung erhoben. Der Datenschutzbeauftragte wird in regelmäßigen Abständen die Datenverarbeitungsvorgänge prüfen und Empfehlungen abgeben. Unter Berücksichtigung der Vorgaben des § 10 HinSchG ist die Verarbeitung der entsprechenden personenbezogenen Daten zulässig und erforderlich. Der bestellte Datenschutzbeauftragte wird die Datenverarbeitung regelmäßig evaluieren.

8. Konsultation der Aufsichtsbehörde

Aufgrund der oben dokumentierten Risikoanalyse stellt der Datenverarbeitungsvorgang kein hohes Risiko für die Betroffenen dar – insbesondere, weil effektive Maßnahmen zur Eindämmung des Risikos getroffen werden konnten.

Eine Konsultation der Aufsichtsbehörde (Landesdatenschutzbeauftragter NRW) ist daher nicht erforderlich.

9. Schlussbemerkung / Unterschriften der Geschäftsführung

Den Risiken wird mit den vorhandenen Sicherheitsmaßnahmen überwiegend in sachgerechter Weise begegnet. Insbesondere wäre eine Anonymisierung nicht geeignet, die Risiken weiter abzusenken, da es den betroffenen Personen im Zusammenhang mit der Zeiterfassung und der u.a. damit einhergehenden arbeitsrechtlichen Dokumentation gerade darauf ankommt, Informationen mit Bezug zu ihrer Person zu erhalten.

Witten, den 24. Januar 2024

Wilhelm Bötzel

