EUROPEAN DATA PROTECTION SUPERVISOR

Leitlinien zur Verarbeitung personenbezogener Informationen im Rahmen eines Verfahrens zur Meldung von Missständen

Juli 2016

Zusammenfassung

Die Meldung von Missständen dient dem Zweck, Korruption aufzudecken. Eine zentrale Herausforderung für die Verhinderung und Bekämpfung von Korruption besteht in der Aufdeckung von Bestechung, Betrug, Diebstahl und anderem Fehlverhalten am Arbeitsplatz. Die Meldung von Missständen ist ein Instrument, um diese Art von unethischem Verhalten ans Licht zu bringen.

Hinweisgeber sind der Ansicht, dass sie im öffentlichen Interesse handeln, wenn sie eine beobachtete schwerwiegende Handlung melden. Leider sind Hinweisgeber häufig mit Vergeltungsmaßnahmen in Form von Schikane, Entlassung, der Erstellung schwarzer Listen und Bedrohungen konfrontiert und ihre Offenlegungen werden regelmäßig ignoriert. Vertraulichkeit ist daher von zentraler Bedeutung und die wirksamste Methode, um Bedienstete zur Meldung von Bedenken zu ermutigen, besteht darin sicherzustellen, dass ihre Identität geschützt ist.

Diese Leitlinien bieten eine praktische Orientierungshilfe für die Organe und Einrichtungen der EU sowohl vor als auch nach der Einführung eines Verfahrens zur Meldung von Missständen, um sicherzustellen, dass dieses mit den in der Verordnung (EG) Nr. 45/2001 festgelegten Datenschutzpflichten in Einklang steht.

Liste der Empfehlungen

Nachstehend findet sich eine Liste der Empfehlungen, auf die in den Leitlinien im Einzelnen eingegangen wird. Der EDSB verwendet diese als Checkliste, wenn er überprüft, ob Sie Ihren in der Verordnung niedergelegten Verpflichtungen nachgekommen sind.

1. Einrichtung festgelegter Kanäle für interne und externe Meldungen sowie spezielle Bestimmungen, in denen der Zweck eindeutig dargelegt ist (S. 4-5).

2. Sicherstellung der Vertraulichkeit der erhaltenen Informationen und Schutz der Identität der Hinweisgeber und aller anderen betroffenen Personen (S. 4-5).

3. Anwendung des Grundsatzes der Datenminimierung: ausschließlich Verarbeitung von personenbezogenen Informationen, die für den konkreten Fall angemessen, relevant und notwendig sind (S. 6).

4. Festlegung, was unter personenbezogenen Informationen in diesem Zusammenhang zu verstehen ist und wer die betroffenen Personen sind, um ihr Recht auf Information, Auskunft und Berichtigung ihrer Daten zu bestimmen. Einschränkungen dieser Rechte sind zulässig, sofern die EU-Organe in der Lage sind, vor dem Treffen einer solchen Entscheidung eine dokumentierte Begründung vorzulegen (S. 6-7).

5. Anwendung des zweistufigen Verfahrens, um jede Gruppe von betroffenen Personen darüber zu informieren, wie ihre Daten verarbeitet werden (S. 7-8).

6. Bei der Beantwortung von Anträgen auf Auskunft Sicherstellung, dass die personenbezogenen Informationen Dritter nicht offengelegt werden (S. 8-9).

7. Bewertung der entsprechenden Zuständigkeit des Empfängers (intern oder extern) und anschließend Beschränkung der Übermittlung von personenbezogenen Informationen ausschließlich auf Fälle, in denen dies für die rechtmäßige Durchführung von Aufgaben im Zuständigkeitsbereich des Empfängers notwendig ist (S. 9).

8. Festlegung angemessener Aufbewahrungsfristen für die im Rahmen des Verfahrens zur Meldung von Missständen verarbeiteten personenbezogenen Informationen, abhängig vom Ergebnis des jeweiligen Falls (S. 9-10).

9. Einführung organisatorischer und technischer Sicherheitsmaßnahmen auf der Grundlage einer Risikobewertung/-analyse des Verfahrens zur Meldung von Missständen, um eine rechtmäßige und sichere Verarbeitung personenbezogener Informationen sicherzustellen (S. 10-11).

INHALTSVERZEICHNIS

1. EINLEITUNG

1 Verfahren zur Meldung von Missständen sollen sichere Kanäle für jeden bereitstellen, der Kenntnis von möglichen Fällen von Betrug, Korruption oder anderen schweren Missständen und Unregelmäßigkeiten erlangt und diese meldet. Hinweisgeber sind der Ansicht, dass sie im öffentlichen Interesse handeln, wenn sie eine beobachtete schwerwiegende Handlung melden.

2 Im Statut der Beamten der Europäischen Union („Statut“) und in den Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union („BBSB“)[1] ist für Bedienstete der EU-Organe und -Einrichtungen („EU-Organe“) und alle Personen, die für diese tätig sind, die Pflicht festgeschrieben, schriftlich jeden begründeten Verdacht von unrechtmäßigen Handlungen den Vorgesetzten oder direkt dem Europäischen Amt für Betrugsbekämpfung („OLAF“) zu melden. Einige EU-Organe haben überdies interne Vorschriften für die Meldung von Missständen durch ihre Bediensteten angenommen. Da die Regelungen zur Meldung von Missständen als Mechanismus zur Aufdeckung von Fällen und zu ihrer Meldung an das OLAF dienen, betrifft die Pflicht zur Meldung nur schwerwiegende Missstände und Unregelmäßigkeiten. Der Anwendungsbereich dieser Leitlinien ist auf die Anfangsphase, wenn die EU-Organe eine Meldung erhalten, beschränkt und sie finden keine Anwendung, wenn ein Fall direkt an das OLAF verwiesen oder übermittelt wird.

3 Verfahren zur Meldung von Missständen umfassen die Verarbeitung sensibler personenbezogener Informationen. Die EU-Organe müssen Berichte über die Meldung von Missständen bearbeiten und den Schutz der personenbezogenen Informationen der Hinweisgeber, der sich mutmaßlich fehlverhaltenden Person, der Zeugen und anderer in dem Bericht genannten Personen sicherstellen. In den vorliegenden Leitlinien wird erläutert, wie die Datenschutzgrundsätze in diesem konkreten Zusammenhang, der das Privatleben der betreffenden Personen beeinflussen kann, anzuwenden sind, und dies anhand hypothetischer Beispiele verdeutlicht. Die Leitlinien zeigen zudem auf, dass die Datenschutzgrundsätze zur Stärkung der Verfahren zur Meldung von Missständen angewandt werden können. Indem die Sicherheitsaspekte des Verfahrens gestärkt werden, trägt die Anwendung der Datenschutzgrundsätze unter anderem dazu bei, zuverlässige Kanäle zu schaffen.

4 Externe Parteien, die mit den EU-Organen einen Vertrag schließen oder mit ihnen in Kontakt treten (wie Berater, Auftragnehmer, Wissenschaftler usw.), sollten darüber informiert werden, dass es möglich ist, einen Verdacht auf Betrug, Korruption oder andere schwerwiegende Missstände oder Unregelmäßigkeiten zu melden.

5 Dieser Verarbeitungsvorgang ist vermutlich mit besonderen Risiken verbunden[2] und unterliegt deshalb der Vorabkontrolle durch den Europäischen Datenschutzbeauftragten („EDSB“).

[1] Der allgemeine Rechtsrahmen für die EU-Bediensteten, die als Hinweisgeber auftreten, ist in den Artikeln 22 a, 22 b und 22 c des Statuts festgelegt, die nach Artikel 11 der Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union für Bedienstete, die auf Vertragsbasis tätig sind, sinngemäß gelten.
[2] Artikel 27 Absatz Buchstaben a und b der Verordnung (EG) Nr. 45/2001 (die „Verordnung“).

2. SICHERE KANÄLE FÜR DIE MELDUNG VON BETRUG – GEWÄHRLEISTUNG VON VERTRAULICHKEIT

6 Die wirksamste Methode, um Bedienstete zur Meldung von Bedenken zu ermutigen, besteht darin sicherzustellen, dass ihre Identität geschützt ist. Deshalb sollten klar definierte Kanäle für interne und externe Meldungen vorhanden sowie der Schutz der erhaltenen Informationen gewährleistet sein. Die Identität des Hinweisgebers, der schwerwiegende Missstände oder Unregelmäßigkeiten nach Treu und Glauben meldet, sollte streng vertraulich behandelt werden, da er vor Vergeltungsmaßnahmen geschützt werden sollte. Abgesehen von bestimmten Ausnahmefällen, in denen Hinweisgeber zu einer solchen Offenlegung einwilligt, dies für ein anschließendes Strafverfahren erforderlich ist oder in denen der Hinweisgeber in böswilliger Absicht eine falsche Aussage macht, darf die Identität des Hinweisgebers niemals offengelegt werden. Im letzten Fall dürfen diese personenbezogenen Daten ausschließlich den Justizbehörden offengelegt werden.[3] Eine Aussage ist böswillig, wenn der Hinweisgeber Handlungen meldet, von denen er weiß, dass sie nicht zutreffend sind. Wenn ein EU-Organ Kenntnis erlangt, dass einem Hinweisgeber bekannt war, dass die von ihm vorgebrachten Vorwürfe unbegründet waren, obliegt es dem Organ, die Böswilligkeit der Vorwürfe nachzuweisen.

7 Die beschuldigte Person sollte genauso wie der Hinweisgeber geschützt werden, da die Gefahr einer Stigmatisierung und Viktimisierung innerhalb ihrer Organisation besteht. Sie werden derartigen Risiken schon ausgesetzt, bevor sie überhaupt wissen, dass Beschuldigungen gegen sie erhoben werden und dass die behaupteten Sachverhalte daraufhin untersucht wurden, ob sie der Wahrheit entsprechen.

8 Deshalb darf ein interner Zugang zu den im Rahmen der Untersuchung der Vorwürfe verarbeiteten Informationen ausschließlich nach dem Grundsatz des berechtigten Informationsinteresses („Need-to-know"), d. h. in Anhängigkeit von der Notwendigkeit eines Zugangs, gewährt werden. Die für die Bearbeitung der Berichte zuständigen Personen könnten beispielsweise einer zusätzlichen Geheimhaltungspflicht unterliegen. Zudem müssen personenbezogene Daten sicher gespeichert werden (siehe Sicherheitsmaßnahmen).

9 Mit der Meldung von Missständen in Zusammenhang stehende personenbezogene Informationen, die für statistische Zwecke gespeichert werden, sollten anonymisiert werden. Die EU-Organe (besonders kleinere EU-Organe) sollten bei Informationen, die zu einer *indirekten* Identifizierung führen können, mit besonderer Vorsicht vorgehen. Beispielsweise könnte die Speicherung der Art einer Meldung von Missständen zusammen mit der Staatsangehörigkeit des Hinweisgebers zu einer indirekten Identifizierung führen und sollte deshalb vermieden werden.

Beispiel 1: *In einer EU-Agentur gelten explizite Empfehlungen für ihre Bediensteten, wie die Vertraulichkeit von Hinweisgebern und der sich mutmaßlich fehlverhaltenden Person während der Erstbewertung eines Falles zu garantieren ist. Der EDSB betont, dass die Gefährdung der betreffenden Parteien gleich ist, ungeachtet, ob der Fall abgeschlossen oder noch nicht abgeschlossen ist. Der Schutz von Hinweisgebern und der sich mutmaßlich*

[3] Siehe EDSB Fall 2010-0458.

3. VERMEIDUNG EINES MISSBRAUCHS DES VERFAHRENS – FESTLEGUNG DES ZWECKS

10 Der Anwendungsbereich des Verfahrens muss begrenzt sein, um einen Missbrauch des Verfahrens zu vermeiden. Der Zweck des Verfahrens zur Meldung von Missständen muss[4] in den internen Vorschriften/der Strategie der EU-Organe **eindeutig dargelegt** sein. In den internen Vorschriften oder einer Strategie sollte explizit beschrieben werden, unter welchen Umständen Kanäle zur Meldung von Missständen genutzt werden müssen und unter welchen Umständen dies nicht notwendig ist. Generell **sollten** die Kanäle zur Meldung von Missständen **nicht verwendet werden**, wenn die Bediensteten ihre gesetzlichen Rechte ausüben, d. h. im Zuge der Einreichung eines Antrags oder einer Beschwerde bei der Anstellungsbehörde gemäß Artikel 90 des Statuts oder bei Belästigungsfällen und persönlichen Differenzen, bei denen sich die Bediensteten selbst an die Personalabteilung, die Mediationsstelle oder eine Vertrauensperson wenden bzw. einen Antrag auf Beistand gemäß Artikel 24 des Statuts einreichen können.

11 In den internen Vorschriften oder in einer Strategie sollte des Weiteren dargelegt werden, dass sensible Informationen, wie rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit sowie Daten über den Gesundheitszustand oder das Sexualleben[5], die für den Fall nicht relevant sind, vermieden werden sollten. Dies wird dazu beitragen, die Erhebung zu vieler personenbezogener Informationen zu vermeiden (siehe unten).

12 Grundsätzlich sollten **Meldungen von Missständen nicht anonym erfolgen.** Hinweisgeber sollten aufgefordert werden, sich selbst zu identifizieren, nicht nur um einen Missbrauch des Verfahrens zu vermeiden, sondern auch um ihren wirksamen Schutz vor Vergeltungsmaßnahmen sicherzustellen. Zudem wird dadurch eine bessere Bearbeitung des Vorgangs ermöglicht, sollten weitere Informationen erforderlich sein.

4. VERMEIDUNG DER VERARBEITUNG ZU VIELER PERSONENBEZOGENER INFORMATIONEN

13 Manchmal kommen die EU-Organe in den Besitz personenbezogener Informationen, die eindeutig ohne Belang oder Bedeutung für die Vorwürfe sind. **Solche Informationen sollten nicht weiter verarbeitet werden.** Dies ist vor allem für besondere Kategorien von Informationen von Bedeutung. Alle für die Untersuchung zuständigen Personen sollten von dieser Regel in Kenntnis gesetzt werden.

> ***Beispiel 2:*** *Ein Hinweisgeber meldet, ein Kollege habe eine betrügerische Handlung begangen. Im Rahmen seiner Aussage legt der Hinweisgeber Informationen über den Gesundheitszustand seines Kollegen offen. Für das Organ ist offensichtlich, dass diese Informationen für das gemeldete Fehlverhalten völlig ohne Bedeutung sind und diese daher nicht weiter zu verarbeiten oder an den Absender zurückzusenden sind.*

[4] Artikel 4 Absatz 1 Buchstabe b der Verordnung.
[5] Artikel 10 Absatz 1 der Verordnung.

14 Es hat sich bewährt, beispielsweise in die internen Verfahrensvorschriften eine allgemeine Empfehlung einzuführen, nämlich die mit den Vorgängen befassten Personen an die Regeln für die Datenqualität[6] zu erinnern und ihnen zu empfehlen, für die Einhaltung dieser Regeln zu sorgen.

5. BESTIMMUNG, WAS IN DIESEM ZUSAMMENHANG UNTER PERSONENBEZOGENEN INFORMATIONEN ZU VERSTEHEN IST

15 Personenbezogene Informationen werden definiert als alle Informationen über eine bestimmte oder bestimmbare natürliche Person.[7] Personenbezogene Informationen umfassen nicht nur Informationen über das Privat- und Familienleben einer Person, sondern auch Informationen bezüglich der Tätigkeiten einer Person, wie etwa ihre Arbeitsbeziehungen und ihr wirtschaftliches und soziales Verhalten[8]. Dies ist beispielsweise beim Abstecken des Umfangs des Rechts der betroffenen Person auf Auskunft zu bedenken. In den meisten Fällen umfassen personenbezogene Daten Angaben zur Identifizierung (z. B. Kontaktangaben), aber auch Informationen zum Verhalten einer Person.

Beispiel 3: *Der Bericht des Hinweisgebers umfasst Informationen, mit denen die sich mutmaßlich fehlverhaltende Person und Zeugen identifiziert werden. Beim eigentlichen Bericht handelt es sich ebenfalls um personenbezogene Informationen des Hinweisgebers, da er sich auf sein Verhalten (als Hinweisgeber) bezieht.*

16 Die gleichen Informationen können sich gleichzeitig auf mehrere Personen beziehen. Möglicherweise enthält der Bericht des Hinweisgebers personenbezogene Informationen über Zeugen oder Dritte (Personen, die in der Akte nur genannt werden), die beschuldigten Personen und den Hinweisgeber selbst.

17 Andererseits hat allein die Tatsache, dass ein Name in einem Dokument erwähnt wird, nicht zwangsläufig zur Folge, dass es sich bei allen in dem Dokument enthaltenen Informationen um „Daten zu dieser Person“ handelt. In vielen Fällen können Informationen nur dann als personenbezogen gelten, wenn sie sich auf die betreffende Person beziehen.

Beispiel 4: *Ein EU-Organ hat möglicherweise einen Bericht zur Prüfung erstellt, ob der Fall an das OLAF zu verweisen ist oder nicht. Die Untersuchung kann sich auf den Hinweisgeber als Quelle beziehen, allerdings handelt es sich nicht bei dem gesamten Bericht um personenbezogene Informationen über den Hinweisgeber.*

[6] Artikel 4 Absatz 1 der Verordnung.
[7] Artikel 2 Buchstabe a der Verordnung.
[8] Artikel 29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, WP 136, angenommen am 20. Juni 2007.

6. UNTERRICHTUNG JEDER GRUPPE VON BETROFFENEN PERSONEN

18 Informationen zu Verfahren zur Meldung von Missständen sollten den Beteiligten in einer sehr deutlichen Weise zur Verfügung gestellt werden, wozu ein **zweistufiges** Verfahren erforderlich ist. Zwar ist die Veröffentlichung einer Datenschutzerklärung auf der Website (oder im Rahmen eines öffentlichen oder internen Dokuments) sicherlich ein positiver Schritt, doch ist dies nach Auffassung des Datenschutzbeauftragten **nicht ausreichend**, da die Informationen übersehen werden könnten. Allen von einem bestimmten Verfahren zur Meldung von Missständen betroffenen Personen sollte zudem so bald wie möglich direkt eine spezielle Datenschutzerklärung bereitgestellt werden, beispielsweise per E-Mail. Zu den betroffenen Personen zählen in der Regel die Hinweisgeber, Zeugen, Dritte (Bedienstete oder andere Personen, die nur erwähnt werden) sowie die beschuldigte Person bzw. die beschuldigten Personen.

6.1. Unterrichtung des Hinweisgebers (Artikel 11 der Verordnung)

19 In diesem Zusammenhang ist es wichtig, über mögliche Empfänger oder Gruppen von Empfängern[9] der personenbezogenen Informationen des Hinweisgebers zu informieren. Darüber hinaus sollte die Datenschutzerklärung auch Informationen über die Folgen einer missbräuchlichen Verwendung (wenn der Hinweisgeber böswillig eine falsche Aussage macht) des Verfahrens zur Meldung von Missständen enthalten, z. B. Disziplinarmaßnahmen.

6.2. Unterrichtung der sich mutmaßlich fehlverhaltenden Person (Artikel 12 der Verordnung)

20 In bestimmten Fällen kann die Unterrichtung der beschuldigten Person in einer frühen Phase für den Fall nachteilig sein. In diesen Fällen könnte die Bereitstellung von spezifischen Informationen aufgeschoben werden müssen..[10] Über einen Aufschub bei der Bereitstellung von Informationen sollte im Einzelfall entschieden werden. Die Gründe für eine Einschränkung sollten dokumentiert werden und dem EDSB auf Ersuchen im Rahmen einer Überwachungs- und Durchsetzungsmaßnahme vorgelegt werden. Diese Gründe sollten beispielsweise belegen, dass ein hohes Risiko besteht, dass bei der Gewährung von Auskunft das Verfahren beeinträchtigt würde oder die Rechte und Freiheiten der übrigen Personen untergraben würden. Die Gründe sollten dokumentiert werden, bevor die Entscheidung über die Anwendung einer Einschränkung oder einen Aufschub getroffen wird.

6.3. Unterrichtung von Zeugen (Artikel 11 der Verordnung)

21 Den Zeugen sollten so bald wie möglich spezifische Informationen bereitgestellt werden, beispielsweise bevor sie von dem Organ befragt werden.

6.4. Unterrichtung von Dritten (Artikel 12 der Verordnung)

22 Je nach Fall kann die Unterrichtung der in einem Bericht über die Meldung von Missständen erwähnten Dritten mit einem unverhältnismäßigen Aufwand verbunden

[9] Artikel 11 Absatz 1 Buchstabe c der Verordnung.
[10] Artikel 20 der Verordnung.

sein.[11] Die Bewertung, ob der Aufwand für die Unterrichtung von Dritten unverhältnismäßig ist oder nicht, muss im Einzelfall vorgenommen werden. Darüber hinaus würde in bestimmten Fällen die Unterrichtung von Personen einen zusätzlichen Verarbeitungsvorgang darstellen, der einschneidender sein kann als der erste Vorgang.

Beispiel 5:
a) Ein Hinweisgeber fügt dem Bericht eine Liste der Kunden (200 Personen) eines Hotels bei, um zu belegen, dass die sich mutmaßlich fehlverhaltende Person sich an einem bestimmten Datum in dem Hotel aufgehalten hatte. Die 199 übrigen Kunden stehen mit dem Fall nicht in Verbindung und ihre Informationen werden von dem Organ nicht weiter verarbeitet. Sie sind nicht zu informieren.
b) Ein Hinweisgeber legt zusammen mit dem Bericht einen USB-Stick vor, der den E-Mail-Austausch mit der sich mutmaßlich fehlverhaltenden Person und einigen weiteren Bediensteten enthält. Das Organ führt eine vorläufige Analyse durch und verarbeitet die Informationen der übrigen Bediensteten. Alle betroffenen Bediensteten sollten informiert werden.

7. BEWERTUNG DES AUSKUNFTSRECHTS EINER PERSON UND BESCHRÄNKUNGEN

23 Bei der Prüfung der Auskunftsrechte sollten die Organe den Status des Antragstellers und den aktuellen Stand[12] der Untersuchung berücksichtigen. Der Umfang und die Sensibilität der vorliegenden Informationen (und die etwaig damit verbundenen Risiken bei der Offenlegung) hängen davon ab, ob der Antrag von

- der beschuldigten Person
- dem Hinweisgeber
- einem Zeugen
- oder Dritten gestellt wird.

24 Die Organe müssen eine Einzelfallprüfung vornehmen und die Gründe für ihre Entscheidung dokumentieren. Dabei sollte die Art der vorliegenden Informationen sowie die Tatsache berücksichtigt werden, ob eine der in der Verordnung vorgesehenen Ausnahmen Anwendung findet.

25 **Wenn Auskunft über die personenbezogenen Informationen über eine betroffene Person gewährt wird, sollten die personenbezogenen Informationen über Dritte, wie Informanten, Hinweisgeber oder Zeugen aus dem Dokument entfernt werden.** Eine Ausnahme bilden außergewöhnliche Umstände, wenn der Hinweisgeber einer solchen Offenlegung zustimmt, wenn diese im Rahmen eines anschließenden Strafverfahrens erforderlich ist oder wenn der Hinweisgeber böswillig falsche Angaben gemacht hat. Wenn nach wie vor das Risiko einer Identifizierung von Dritten besteht, sollte die Auskunft aufgeschoben werden. Die Artikel 29-Arbeitsgruppe unterbreitete folgende Empfehlung: „*Die im Bericht eines Informanten beschuldigte Person kann unter keinen*

[11] Artikel 12 Absatz 2 der Verordnung.
[12] Artikel 20 Absatz 1 Buchstabe a der Verordnung.

Umständen auf der Grundlage des Rechts auf Auskunft der beschuldigten Person Informationen zur Identität des Informanten erhalten, es sei denn, dass der Informant böswillig eine falsche Aussage gemacht hätte. In allen anderen Fällen unterliegt die Identität des Informanten stets der Vertraulichkeit.".[13] Dies ist insbesondere von Bedeutung, um sicherzustellen, dass Personen vor potenziellen Risiken geschützt sind, die mit der Offenlegung ihrer personenbezogenen Informationen verbunden sind.

Beispiel 6: *Ein EU-Bediensteter, der schwerwiegenden Fehlverhaltens beschuldigt wird, ersucht das Organ um alle personenbezogenen Informationen, die über ihn in Zusammenhang mit den Vorwürfen vorliegen. Ein Großteil dieser Informationen ist in den Aussagen des Hinweisgebers enthalten. Selbst wenn der Name des Hinweisgebers aus diesen Dokumenten gelöscht wird, wäre seine Identität aufgrund des Bezugs zu konkreten Ereignissen, Situationen und beschriebenen Zusammenhängen offensichtlich. Somit sollte das Organ die Offenlegung dieser Informationen mit Blick auf den Schutz der betroffenen Person oder die Rechte und*

8. BESCHRÄNKUNG VON ÜBERMITTLUNGEN

26 Es gelten unterschiedliche Pflichten, die davon abhängig sind, ob es sich bei dem Empfänger um ein EU-Organ (in diesem Zusammenhang bei der Übermittlung von Daten durch ein Organ an das OLAF) oder eine der Richtlinie 95/46/EG unterliegende Personen (wie ein nationales Gericht oder andere Arten von Empfängern) handelt.[14] **Die Anforderungen für die Übermittlung von Daten müssen im Einzelfall bewertet werden.** Insbesondere sollten personenbezogene Informationen nur übermittelt werden, wenn es für die rechtmäßige Erfüllung der in den Zuständigkeitsbereich des Empfängers fallenden Aufgaben erforderlich ist.

9. FESTLEGUNG VON AUFBEWAHRUNGSFRISTEN IN ABHÄNGIGKEIT VOM ERGEBNIS DES FALLES

27 Personenbezogene Information dürfen nicht länger aufbewahrt werden, als es mit Blick auf den Zweck der Verarbeitung erforderlich ist.[15] Deshalb sollten unterschiedliche Aufbewahrungsfristen gelten, die von den Informationen im Bericht und der Bearbeitung des Falles abhängen.

28 Erstens sollten, wie oben erwähnt, personenbezogene Informationen, die für die Vorwürfe nicht von Belang sind, nicht weiter verarbeitet werden (siehe Absatz 4).

29 Zweitens gilt für den Fall, dass eine Erstbewertung vorgenommen wird, sich aber herausstellt, dass der Fall nicht an das OLAF weiterzuleiten ist oder nicht in den Anwendungsbereich des Verfahrens zur Meldung von Missständen fällt, dass der Bericht so bald wie möglich gelöscht werden sollte (oder an den richtigen Kanal weitergeleitet

[13] Artikel 29 Datenschutzgruppe, Stellungnahme zur Anwendung der EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität, WP 117, angenommen am 1. Februar 2006, S. 14

[14] Artikel 7, 8 und 9 der Verordnung.

[15] Artikel 4 Absatz 1 Buchstabe e der Verordnung.

werden sollte, wenn es sich beispielsweise um eine angebliche Belästigung handelt). In jedem Fall sollten die personenbezogenen Daten unverzüglich und in der Regel innerhalb von zwei Monaten nach Abschluss der vorläufigen Bewertung[16] gelöscht werden, da es unverhältnismäßig wäre, solche sensiblen Informationen weiter zu speichern.

30 Drittens sollte das EU-Organ sorgfältig verfolgen, welche Maßnahmen das OLAF ergreift, sofern sich nach der vorläufigen Bewertung herausstellt, dass der Bericht an das OLAF zu übermitteln ist. Wenn das OLAF eine Untersuchung einleitet, müssen die EU-Organe die Informationen nicht über einen längeren Zeitraum aufbewahren. Sofern das OLAF beschließt, keine Untersuchung einzuleiten, sollten die Informationen unverzüglich gelöscht werden.

31 Sofern eine längere Aufbewahrungsfrist vorgesehen ist, sollte die Auskunft über personenbezogene Daten dennoch beschränkt sein (siehe Sicherheitsmaßnahmen unten). Es hat sich bewährt, diese Berichte vom normalen Fallmanagementsystem/täglich verwendeten System zu trennen.

Beispiel 7: *Ein EU-Organ hat mehrere Berichte über die Meldung von Missständen über den Kanal für die Meldung von Missständen erhalten. Ein Bericht betrifft eine angebliche Belästigung und wird daher direkt an das Referat weitergeleitet, das für diese Fälle zuständig ist. Zwei weitere Berichte betreffen vermutlich Betrug und werden daher an das OLAF weitergeleitet, das in einem der Fälle eine Untersuchung einleitet. Das Organ wendet eine Aufbewahrungsfrist von fünf Jahren für den Bericht an, zu dem das OLAF keine Untersuchung eingeleitet hat. In diesem Fall vertritt der EDSB die Auffassung, dass ein Zeitraum von fünf Jahren unverhältnismäßig ist und der Bericht so bald wie möglich gelöscht werden sollte.*

10. EINFÜHRUNG GEEIGNETER SICHERHEITSMAßNAHMEN

32 Der für die Verarbeitung von Daten Verantwortliche sollte technische und organisatorische Maßnahmen ergreifen, die geeignet sind, ein Schutzniveau zu gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist.[17] Dabei handelt es sich nicht nur um eine eindeutige gesetzliche Pflicht, sondern wie vorstehend erwähnt, ist die Vertraulichkeit bezüglich des gesamten Verfahrens von entscheidender Bedeutung, um die Bediensteten zur Meldung möglicher Bedenken zu ermutigen. Des Weiteren muss bei Sicherheitsmaßnahmen der Sensibilität der verarbeiteten personenbezogenen Informationen Rechnung getragen werden. Vor diesem Hintergrund ist es wesentlich, geeignete Sicherheitsmaßnahmen einzurichten, um wirksam den Zugang von nicht berechtigten Personen zu personenbezogenen Daten zu verhindern und ihre Integrität sicherzustellen.

33 Die Notwendigkeit dieser Sicherheitsmaßnahmen muss unter Berücksichtigung der mit dem **Verfahren zur Meldung von Missständen verbundenen Risiken analysiert werden,** ungeachtet, ob es sich um ein manuelles oder automatisiertes Verfahren handelt: **Es ist eine Risikobewertung der Informationssicherheit durchzuführen.** Nachdem

[16] Artikel 29-Datenschutzgruppe, Stellungnahme 1/2006, WP 117, S. 12.
[17] Siehe Artikel 22 der Verordnung.

die mit den betreffenden personenbezogenen Informationen verbundenen Risiken bestimmt wurden, kann anschließend eine Untersuchung vorgenommen werden, um zu ermitteln, welche Maßnahmen unter Berücksichtigung unter anderem der Kosten dieser Sicherheitsmaßnahmen und ihrer Sichtbarkeit zu ergreifen sind. Da sich die Risiken im Laufe der Zeit verändern, muss das EU-Organ seine Untersuchung, die Auswahl der Sicherheitsmaßnahmen und ihre Wirksamkeit regelmäßig überprüfen.

34 Detaillierte Empfehlungen und Informationen über das Risikomanagement für die Informationssicherheit finden sich in den „Leitlinien für Sicherheitsmaßnahmen für die Verarbeitung personenbezogener Daten – Artikel 22 der Verordnung (EG) Nr. 45/2001“ des EDSB.

Beispiel 8: *Von besonderer Bedeutung für Vorgänge in Zusammenhang mit der Meldung von Missständen:*
a) Der Zugang von Bediensteten zu personenbezogenen Informationen muss strikt auf dem Grundsatz des berechtigten Informationsinteresses („Need-to-know“) beruhen. Bedienstete, die Zugang zu diesen Informationen haben, müssen einer zusätzlichen Geheimhaltungspflicht unterliegen und der Zugang zu Berichten über die Meldung von Missständen muss überwacht werden, sei es in elektronischer Form oder in Papierform.
b) Aus technischer Sicht müssen die allgemeinen Anforderungen der Zugangskontrolle vollständig umgesetzt sein: wirksame Beschränkung und Kontrolle der Personen, die Zugang zu Fällen einer Meldung von Missständen haben, Protokollierung des Zugangs und regelmäßige Überprüfung sowohl des Zugangs als auch der Zugangsrechte.

11. ÜBERNEHMEN SIE VERANTWORTUNG – SIE SIND ZUR RECHENSCHAFT VERPFLICHTET!

35 Rechenschaftspflicht bedeutet, dass Organisationen ihren Datenschutzverpflichtungen nachzukommen haben und auch i**n der Lage sein müssen, dies nachzuweisen.**

36 Die Rechenschaftspflicht ist nicht auf personenbezogene Informationen im Rahmen eines Verfahrens zur Meldung von Missständen beschränkt, sondern gilt für alle Vorgänge, bei denen personenbezogene Informationen verarbeitet werden.

37 Jede Organisation, die personenbezogene Daten erhebt, verwendet und speichert (bezeichnet als Verarbeitung), ist dafür verantwortlich, dass die Datenschutzvorschriften eingehalten werden, und muss über diese Einhaltung Rechenschaft ablegen.

38 Generell müssen die Organe auf transparente Weise und explizit darlegen, wie sie die personenbezogenen Daten im Zusammenhang mit Verfahren zur Meldung von Missständen verarbeiten. Sie müssen ihre Strategien dokumentieren und dafür sorgen, dass die Nutzer von diesen Kenntnis haben. Das Recht auf Schutz der Privatsphäre besteht auch am Arbeitsplatz und die Menschen müssen über das Verfahren informiert werden. Die Organe können nicht einfach davon ausgehen, dass die Bediensteten Bescheid wissen.

39 Am einfachsten kann ein Organ seiner Rechenschaftspflicht nachkommen, wenn es die Datenschutzimplikationen neuer Prozesse schon bei deren Entwurf berücksichtigt

(**eingebauter Datenschutz**). Unterschiedliche Verarbeitungsvorgänge und verschiedene Technologien erfordern unterschiedliche Schutzmaßnahmen. Durch eine Einbeziehung ihres behördlichen Datenschutzbeauftragten schon zu Beginn des Prozesses kann wertvolle Beratung und Orientierung eingeholt werden.

40 Nachstehend eine Liste der wichtigsten zu bedenkenden Aspekte:

a. **Vertraulichkeit:** Wie werden die betroffenen Personen geschützt?

b. **Festlegung des Zwecks:** In welchen Fällen wird der Kanal für die Meldung von Missständen genutzt?

c. **Vermeidung zu vieler Informationen:** Welche Informationen sind für die vorgebrachten Vorwürfe erforderlich?

d. **Festlegung der Bedeutung von personenbezogenen Informationen:** Welches sind personenbezogene Informationen in dem konkreten Bericht?

e. **Unterrichtung jeder Gruppe von betroffenen Personen:** Wer ist von diesem konkreten Bericht betroffen?

f. **Anwendung unterschiedlicher Aufbewahrungsfristen:** Wie lange muss der Bericht aufbewahrt werden?

g. **Durchführung einer Risikobewertung der Informationssicherheit:** Welchen Risiken können Ihre Fälle einer Meldung von Missständen ausgesetzt sein und wie schützen Sie sich dagegen?

41 Der Nachweis der Rechenschaftspflicht impliziert auch die Dokumentation des Verfahrens und seiner Umsetzung. Folgendes sollte dokumentiert werden:

a. eine **Strategie**, **interne Regelungen** oder ein **Beschluss** über die Meldung von Missständen;

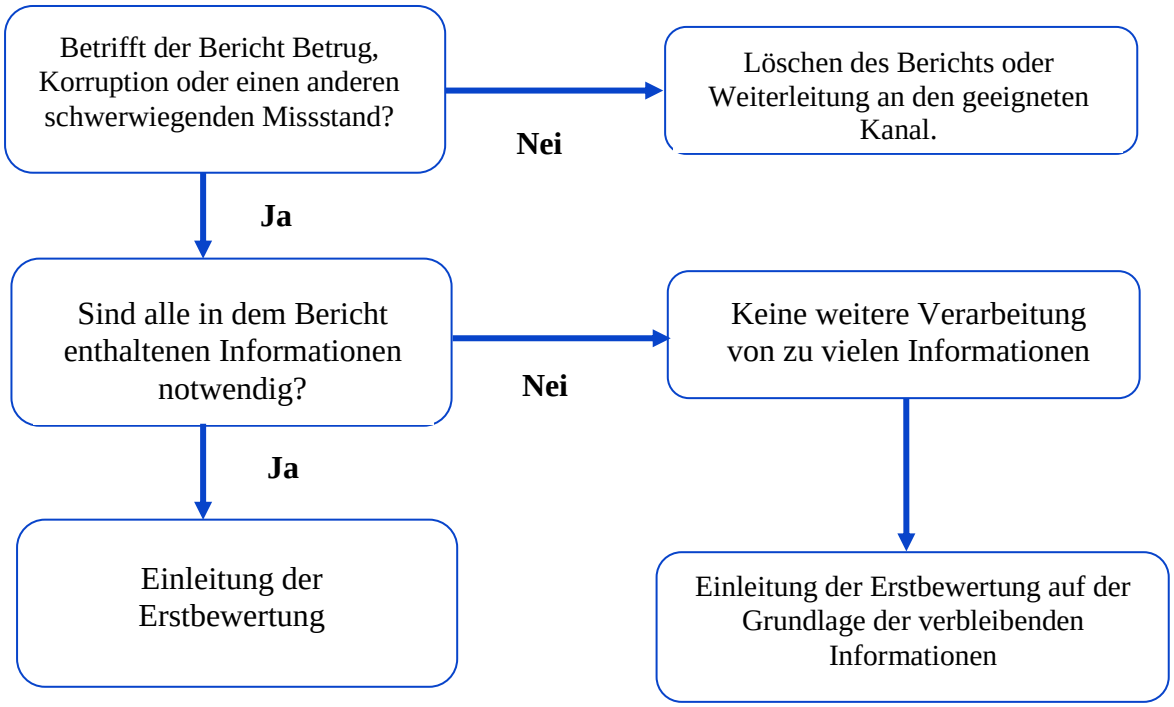
b. die **Beschränkungen des Auskunftsrechts** sollten dokumentiert werden, und zwar nicht nur auf welchen Gründen diese basieren, sondern auch die Begründung, weshalb sie in einer konkreten Situation Anwendung finden;

c. ein **Aufschub bei der Erteilung von Informationen** für die betreffende Person;

d. die für dieses konkrete Verfahren vorgenommene **Risikobewertung**.

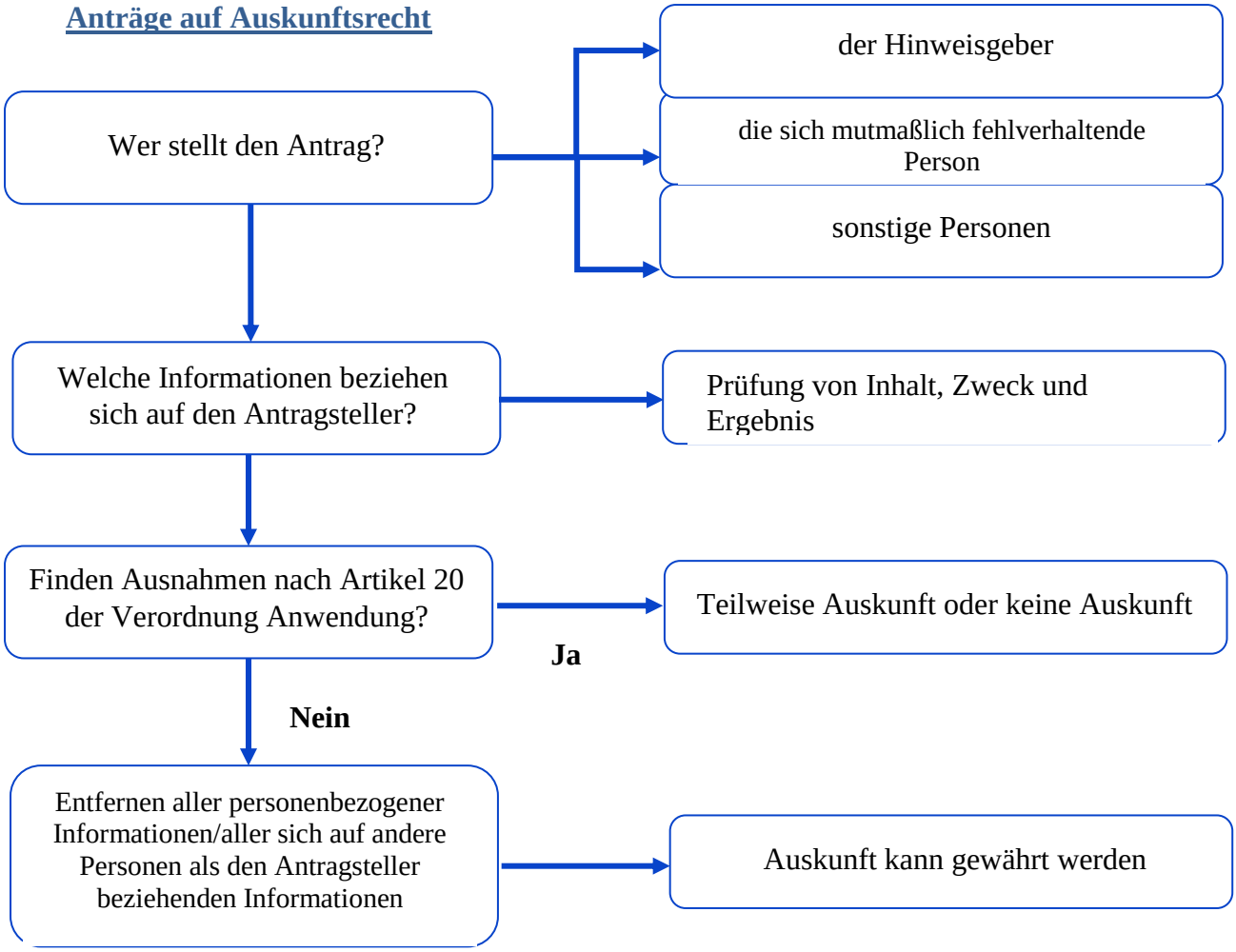
12. FLUSSDIAGRAMME – VERFAHREN ZUR MELDUNG VON MISSSTÄNDEN

12.1. Umgang mit Berichten über die Meldung von Missständen

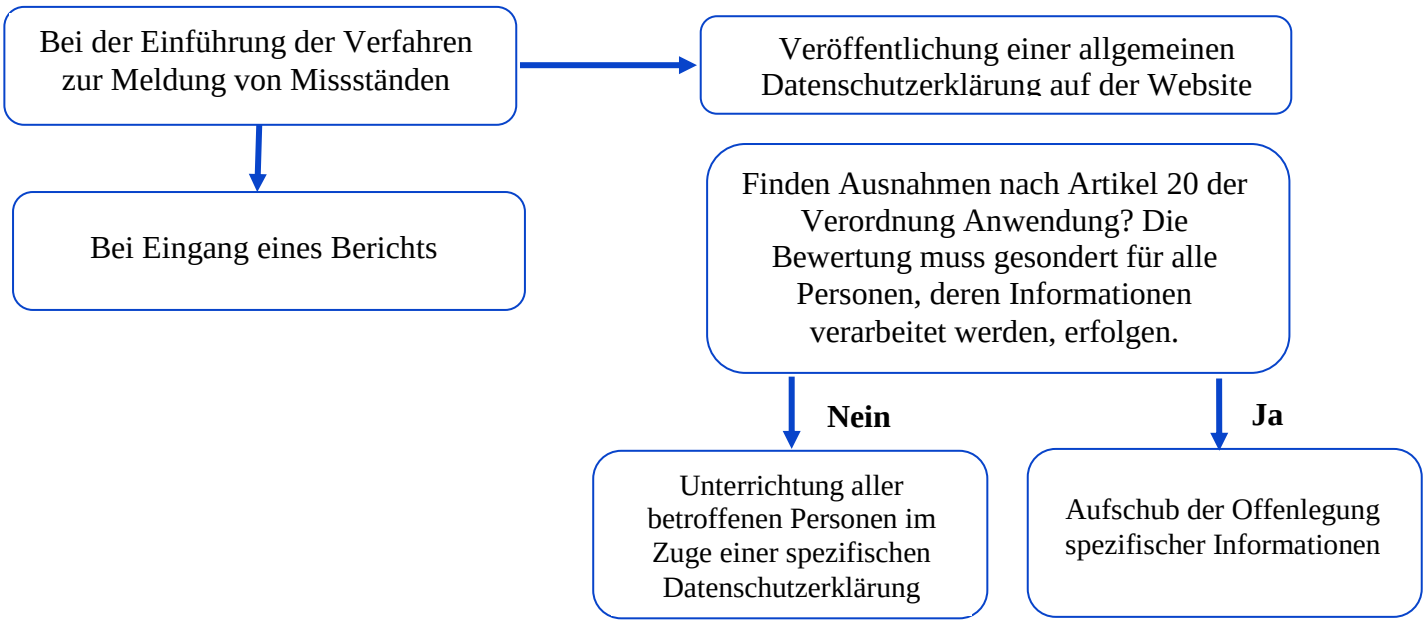


12.2. Sicherstellung der Rechte von Personen

Anträge auf Auskunftsrecht



Angemessene Unterrichtung der Personen



WEITERFÜHRENDE LITERATUR

Beispiele für Stellungnahmen des EDSB

Fall Nr. 2014-0828 – Stellungnahme zum Verfahren für die Meldung von Missständen des Europäischen Bürgerbeauftragten

Fall Nr. 2015-0061 – Stellungnahme zum Verfahren der Exekutivagentur des Europäischen Forschungsrats für den internen Umgang mit und die Meldung von potenziellem Betrug und Unregelmäßigkeiten

Fall Nr. 2015-0349 – Stellungnahme zum Whistleblowing-Verfahren des Generalsekretariats des Rates der Europäischen Union

Fall Nr. 2015-0569 – Stellungnahme zum Verfahren zur Meldung von Missständen („Whistleblowing“) der Europäischen Fischereiaufsichtsagentur (EFCA)

Sonstige Dokumente

Schutz von Whistleblowern – Empfehlung CM/Rec(2014)7 und Erläuternder Bericht – Europarat

Whistleblowing in Europa, Rechtsschutz für Whistleblower in der EU – Transparency International, Internationale Grundsätze für Rechtsvorschriften zu Whistleblowern – Transparency International