DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE (EDSB)

# Leitlinien zur Verarbeitung personenbezogener Daten im Rahmen eines Verfahrens zur Meldung von Missständen („Whistleblowing“)


Dezember 2019

**Zusammenfassung**

Die Meldung von Missständen dient der Aufdeckung von Fehlverhalten oder Korruption. Eine zentrale Herausforderung für die Verhinderung von Korruption besteht in der Aufdeckung von Bestechung, Betrug, Diebstahl und anderem Fehlverhalten am Arbeitsplatz. Durch die Meldung von Missständen wird ein solches unethisches Verhalten ans Licht gebracht.

Da Hinweisgeber mit Repressalien in Form von Schikane, Entlassung, der Erstellung schwarzer Listen und Bedrohungen konfrontiert sein können und/oder ihre Offenlegungen ignoriert werden, schützt das Recht sie vor Vergeltungsmaßnahmen. Vertraulichkeit, einschließlich des Schutzes der Identität, ist daher von zentraler Bedeutung und eine wirksame Methode, um Bedienstete zur Meldung von Bedenken zu ermutigen.

Diese Leitlinien bieten eine praktische Orientierungshilfe für die Organe, Einrichtungen und Agenturen der EU sowohl vor als auch nach der Einführung eines Verfahrens zur Meldung von Missständen, um sicherzustellen, dass dieses mit den in der Verordnung (EU) 2018/1725 festgelegten Datenschutzpflichten in Einklang steht.

Sie aktualisieren die im Juli 2016 veröffentlichten Leitlinien zur Meldung von Missständen.

## 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 bei der Überprüfung, 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. 5).

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

3. Anwendung des Grundsatzes der Datenminimierung: ausschließlich Verarbeitung von personenbezogenen Daten, die für den konkreten Fall angemessen, relevant und notwendig sind (S. 6-7).

4. Festlegung, was unter personenbezogenen Daten in diesem Zusammenhang zu verstehen ist und wer die betroffenen Personen sind, um ihr Recht auf Unterrichtung, Auskunft und Berichtigung ihrer Daten zu bestimmen. Einschränkungen dieser Rechte sind zulässig, sofern die Organe, Einrichtungen und sonstigen Stellen der Union interne Regeln haben und in der Lage sind, vor dem Treffen einer solchen Entscheidung eine dokumentierte Begründung vorzulegen (S. 7).

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

6. Sicherstellung beim Beantworten von Anträgen auf Auskunft, dass die personenbezogenen Daten Dritter nicht offengelegt werden (S. 9-10).

7. Bewertung der entsprechenden Zuständigkeit des Empfängers (intern oder extern) und anschließend Beschränkung der Übermittlung von personenbezogenen Daten ausschließlich auf Fälle, in denen dies für die rechtmäßige Durchführung von Aufgaben im Zuständigkeitsbereich des Empfängers notwendig ist (S. 10).

8. Festlegung angemessener Aufbewahrungsfristen für die im Rahmen des Verfahrens zur Meldung von Missständen verarbeiteten personenbezogenen Daten, abhängig vom Ergebnis des jeweiligen Falls (S. 10-11).

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 Daten sicherzustellen (S. 11-12).

# INHALTSVERZEICHNIS

## 1. EINLEITUNG

1 Verfahren zur Meldung von Missständen („Whistleblowing“) sollen sichere Kanäle für jeden bereitstellen, der Kenntnis von möglichen Fällen von Betrug, Korruption oder anderen schweren Missständen und Unregelmäßigkeiten erlangt und diese meldet. Verfahren zur Meldung von Missständen schützen Hinweisgeber und Offenlegungen, die im öffentlichen Interesse liegen. Sie sind nicht für die Meldung individueller Probleme und Streitigkeiten oder die Einreichung einer Beschwerde gedacht.

2 Diese Leitlinien sollen den Organen, Einrichtungen und sonstigen Stellen der Union (im Folgenden „EU-Institutionen“) für die Praxis Beratung und Anleitung bei der Verarbeitung personenbezogener Daten im Rahmen eines Verfahrens zur Meldung von Missständen geben, um zu gewährleisten, dass sie sich an ihre in der Verordnung (EU) 2018/1725[1] (im Folgenden „Verordnung“) niedergelegten Datenschutzpflichten halten.

3 Der EDSB hat diese Leitlinien auf der Grundlage langjähriger Erfahrung ausgearbeitet. Die erste Ausgabe wurde im Juli 2016 veröffentlicht; zwischenzeitlich wurde die Verordnung (EG) Nr. 45/2001 durch neue Datenschutzvorschriften ersetzt, die für die EU-Institutionen gelten. Die neue Verordnung spiegelt die Datenschutz-Grundverordnung (DSGVO) wider, die für Organisationen in der EU/im EWR gilt. Darüber hinaus wurde eine neue Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden[2] (im Folgenden „Richtlinie“), vereinbart[3]. Diese Leitlinien wurden aktualisiert, um der geltenden Verordnung sowie einigen Elementen dieser Richtlinie Rechnung zu tragen, wenngleich sie auch nicht für EU-Institutionen gilt.

4 Im Statut der Beamten der Europäischen Union (im Folgenden „Statut“) und in den Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union (im Folgenden „BBSB“)[4] ist für Bedienstete und sonstige für die EU-Institutionen tätigen Personen die besondere Pflicht festgeschrieben, jeden begründeten Verdacht von unrechtmäßigen Handlungen den Vorgesetzten oder direkt dem Europäischen Amt für Betrugsbekämpfung (im Folgenden „OLAF“) schriftlich zu melden. Die EU-Institutionen 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-Institutionen eine Meldung erhalten, beschränkt und sie finden keine Anwendung, wenn ein Fall an das OLAF verwiesen oder direkt übermittelt wird.

5 Bei Verfahren zur Meldung von Missständen werden besondere Datenkategorien verarbeitet. Die EU-Institutionen müssen Berichte über die Meldung von Missständen

[1] ABl. L 295/39 vom 21.11.2018
[2] Richtlinie des Europäischen Parlaments und des Rates zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, 2018/0106 (COD).
[3] Der Rechtsakt wird nun förmlich unterzeichnet und im Amtsblatt veröffentlicht werden.
[4] Der allgemeine Rechtsrahmen für die EU-Bediensteten, die als Hinweisgeber handeln, ist in den Artikeln 22a, 22b und 22c des Statuts festgelegt, die nach Artikel 11 der Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union auf Vertragsbedienstete entsprechend Anwendung finden.

bearbeiten und den Schutz der personenbezogenen Daten 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 somit dazu bei, zuverlässige Kanäle zu schaffen.

6 Externe Parteien, die mit den EU-Institutionen 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.

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

7 Die wirksamste Methode, um Mitarbeiter 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 Repressalien geschützt werden sollte. Abgesehen von bestimmten Ausnahmefällen, in denen der 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.[5] Eine Aussage ist böswillig, wenn der Hinweisgeber Handlungen meldet, von denen er weiß, dass sie nicht zutreffend sind. Wenn eine EU-Institution feststellt, dass ein Hinweisgeber einen unbegründeten Vorwurf vorgebracht hat, obliegt es dem Organ, die Böswilligkeit der Anschuldigungen nachzuweisen.

8 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.

9 Meldungen über Missstände können auch personenbezogene Daten über Dritte wie etwa Zeugen oder Kollegen enthalten. Ihre personenbezogenen Daten sollten ebenfalls in allen Phasen des Verfahrens geschützt werden.[6]

[5] Siehe EDSB-Fall 2010-0458.
[6] Erwägungsgrund 76 der Richtlinie.

10 Deshalb darf ein interner Zugang zu den im Rahmen der Untersuchung der Vorwürfe verarbeiteten Informationen ausschließlich nach dem Grundsatz des berechtigten Informationsinteresses gewährt werden, d. h. nur im jeweils notwendigen Umfang. Die für die Bearbeitung der Berichte zuständigen Personen könnten beispielsweise einer zusätzlichen Geheimhaltungspflicht unterliegen. Zudem müssen personenbezogene Daten sicher gespeichert werden (siehe Sicherheitsmaßnahmen).

11 Mit der Meldung von Missständen in Zusammenhang stehende personenbezogene Daten, die zu statistischen Zwecke gespeichert werden, sollten anonymisiert werden. Die EU-Institutionen (besonders kleinere EU-Institutionen) 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 beteiligten Parteien gleich ist, ungeachtet, ob der Fall abgeschlossen oder noch nicht abgeschlossen ist. Der Schutz von Hinweisgebern und der sich mutmaßlich fehlverhaltenden Personen sollte deshalb auch nach Abschluss eines Falles in Betracht gezogen werden.*

## 3. VERMEIDUNG EINES MISSBRAUCHS DES VERFAHRENS – FESTLEGUNG DES ZWECKS

12 Der Anwendungsbereich des Verfahrens muss begrenzt sein, um einen Missbrauch des Verfahrens zu vermeiden. Der Zweck des Verfahrens zur Meldung von Missständen muss in den internen Vorschriften / der Strategie der EU-Institutionen **eindeutig dargelegt**[7] 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 diese Kanäle nicht genutzt werden sollten. 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.

13 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[8], die für den Fall nicht relevant sind, nicht in den Akten erfasst werden

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

sollten. Dies wird dazu beitragen, die Erhebung zu vieler personenbezogener Daten zu vermeiden (siehe unten, Abschnitt 4).

14 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 Repressalien sicherzustellen. Dies wird zudem die Verwaltung der Akte erleichtern, wenn zusätzliche Informationen eingeholt werden müssen.

## 4. VERMEIDUNG DER VERARBEITUNG ZU VIELER PERSONENBEZOGENER DATEN

15 Manchmal kommen die EU-Institutionen in den Besitz personenbezogener Daten, 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 einen Betrug 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.*

16 Es hat sich bewährt, eine allgemeine Empfehlung einzuführen, beispielsweise in den internen Verfahrensvorschriften die mit den Vorgängen im Zusammenhang mit der Meldung von Missständen befassten Personen an die Einhaltung der Regeln für die Datenqualität zu erinnern[9]. Ein weiteres bewährtes Verfahren, das in der Richtlinie festgelegt ist[10], wäre die Bereitstellung von Datenschutzschulungen für die Mitarbeiter, die für die Bearbeitung von Meldungen zuständig sind.

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

17 Personenbezogene Daten werden definiert als alle Informationen über eine bestimmte oder bestimmbare natürliche Person[11]. Personenbezogene Daten 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[12]. Dies ist beispielsweise beim Abstecken des Umfangs des Rechts der betroffenen Person auf Auskunft zu bedenken. In den meisten

[9] Artikel 4 Absatz 1 der Verordnung.
[10] Erwägungsgrund 74 der Richtlinie.
[11] Artikel 3 Absatz 1 der Verordnung.
[12] Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, WP 136, angenommen am 20. Juni 2007.

Fällen umfassen personenbezogene Daten Angaben zur Identifizierung (z. B. Kontaktangaben), aber auch Informationen zum Verhalten dieser 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 Daten des Hinweisgebers, da er sich auf sein Verhalten (als Hinweisgeber) bezieht.*

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

19 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:*** *Eine EU-Institution 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 Daten über den Hinweisgeber.*

## 6. UNTERRICHTUNG JEDER GRUPPE VON BETROFFENEN PERSONEN

20 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) ein positiver Schritt, doch ist dies nach Auffassung des Europäischen Datenschutzbeauftragten **nicht ausreichend**, da die Informationen übersehen werden könnten. Allen von einem bestimmten Verfahren zur Meldung von Missständen betroffenen Personen sollte 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 15 der Verordnung)

21 In diesem Zusammenhang ist es wichtig, sämtliche Personen, die von dem Vorgang betroffen sind, darüber zu informieren, an wen ihre personenbezogenen Daten weitergegeben werden (potenzielle Empfänger oder Kategorien von Empfängern[13]).

[13] Artikel 15 Absatz 1 Buchstabe d der Verordnung.

Darüber hinaus sollten sie im Datenschutzhinweis auch über die Folgen des Missbrauchs des Verfahrens zur Meldung von Missständen (z. B. wenn der Hinweisgeber böswillig eine falsche Aussage macht) informiert werden, wie etwa Disziplinarmaßnahmen.

## 6.2 Unterrichtung der sich mutmaßlich fehlverhaltenden Person (Artikel 16 der Verordnung)

22 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 eingeschränkt werden müssen.[14] EU-Institutionen müssen über interne Vorschriften verfügen, um Informationen einschränken zu können (siehe Absatz 26). 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 15 der Verordnung)

23 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 16 der Verordnung)

24 Je nach Fall kann die Unterrichtung der in einem Bericht über die Meldung von Missständen erwähnten Dritten mit einem unverhältnismäßigen Aufwand verbunden sein.[15] 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 stärker in die Privatsphäre eingreifen könnte als der ursprüngliche 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.*

[14] Artikel 25 der Verordnung.
[15] Artikel 16 Absatz 5 Buchstabe b der Verordnung.

*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

25 Bei der Prüfung der Auskunftsrechte sollten die EU-Institutionen den Status des Antragstellers und den Stand[16] 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.

26 EU-Institutionen sollten sicherstellen, dass eine klare Rechtsgrundlage vorhanden ist, bevor Beschränkungen gemäß Artikel 25 der Verordnung angewendet werden. Das bedeutet, dass EU-Institutionen interne Vorschriften für Ausnahmefälle, in denen die Unterrichtung zurückgestellt werden könnte, erlassen sollten. Darüber hinaus muss vor der Anwendung einer Beschränkung in einem bestimmten Fall eine Prüfung der Notwendigkeit und Verhältnismäßigkeit stattfinden, und die EU-Institutionen müssen die Gründe für ihre Entscheidung dokumentieren, um ihrer Rechenschaftspflicht nachzukommen. Weitere Informationen über interne Vorschriften und die Bewertung im Einzelfall finden Sie in den Leitlinien des EDSB zu Artikel 25 der neuen Verordnung und den internen Vorschriften. Darüber hinaus müssen EU-Institutionen möglicherweise zwischen einer internen Begründung für die Anwendung der Einschränkung und einer allgemeinen Begründung, über die der Antragsteller gemäß Artikel 25 Absatz 6 zu unterrichten ist, unterscheiden, es sei denn, diese Unterrichtung kann gemäß Artikel 25 Absatz 8 zurückgestellt werden.

[16] Artikel 25 Absatz 1 Buchstaben b und f der Verordnung.

***Beispiel 6:*** *Ein Hinweisgeber (A) meldet den Verdacht eines Betruges durch einen Kollegen und Vorgesetzten (B). Nach Abschluss der Untersuchung beantragt B Auskunft über ihre zu diesem Zweck verarbeiteten personenbezogenen Daten. Die Behauptungen von A enthalten zum Teil personenbezogene Daten von B. Die EU-Institution kann möglicherweise eine Beschränkung gemäß Artikel 25 Absatz 1 Buchstabe h aufgrund der Tatsache rechtfertigen, dass A die Daten bereitgestellt hat, und wenn davon ausgegangen werden kann, dass A diese Informationen bereitgestellt hat, könnte A Repressalien von B ausgesetzt sein. Dies müsste intern dokumentiert werden. Natürlich sollte B nicht mitgeteilt werden, dass der Grund für die Beschränkung darin besteht, dass A Repressalien erleiden könnte, da sie die Wirkung der Beschränkung gemäß Artikel 25 Absatz 8 zunichtemachen würde. Daher müssten die B gemäß Artikel 25 Absatz 6 übermittelten Informationen allgemeiner formuliert werden.*

27 **Wenn Auskunft über die personenbezogenen Daten über eine betroffene Person gewährt wird, sollten die personenbezogenen Daten 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[17] 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 Richtlinie sieht das Gebot der Vertraulichkeit vor (Artikel 16 Absatz 1), wonach die Mitgliedstaaten verpflichtet sind, sicherzustellen, dass die Identität des Hinweisgebers ohne dessen ausdrückliche Zustimmung keinen anderen Personen als gegenüber den befugten Mitarbeitern offengelegt wird. Dies ist insbesondere von Bedeutung, um sicherzustellen, dass Personen vor potenziellen Risiken geschützt sind, die mit der Offenlegung ihrer personenbezogenen Daten verbunden sind.

***Beispiel 7:*** *Ein EU-Bediensteter, der schwerwiegenden Fehlverhaltens beschuldigt wird, ersucht das Organ um alle personenbezogenen Daten, 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 Freiheiten anderer Personen aufschieben (Artikel 25 Absatz 1 Buchstabe h), sofern dies in den internen Vorschriften der EU-Institution festgelegt ist.*

## 8. BESCHRÄNKUNG VON ÜBERMITTLUNGEN

[17] Nach Artikel 16 Absatz 2 der Richtlinie *[darf] die Identität … jedoch nur dann offengelegt werden, wenn dies nach Unionsrecht oder nationalem Recht eine notwendige und verhältnismäßige Pflicht im Rahmen der Untersuchungen durch nationale Behörden oder von Gerichtsverfahren darstellt – auch im Hinblick auf die Verteidigungsrechte der betroffenen Person.*

28 Es gelten unterschiedliche Pflichten, die davon abhängig sind, ob es sich bei dem Empfänger um eine EU-Institution handelt (im vorliegenden Zusammenhang ist das bei der Übermittlung von Daten durch eine Institution an das OLAF der Fall) oder ein der DSGVO unterliegender Empfänger (wie ein nationales Gericht oder andere Arten von Empfängern).[18] **Die Anforderungen für die Übermittlung von Daten müssen im Einzelfall bewertet werden.** Insbesondere sollten personenbezogene Daten 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

29 Personenbezogene Information dürfen nicht länger aufbewahrt werden, als es mit Blick auf den Zweck der Verarbeitung erforderlich ist.[19] Deshalb sollten unterschiedliche Aufbewahrungsfristen gelten, die von den Informationen im Bericht und der Bearbeitung des Falles abhängen:

30 Personenbezogene Daten, die für die Vorwürfe nicht relevant sind, sollten nicht weiter verarbeitet und unverzüglich gelöscht werden[20] (siehe Abschnitt 4).

31 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, gilt, dass der Bericht so bald wie möglich gelöscht werden sollte (oder an den richtigen Kanal weitergeleitet 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 gelöscht werden[21], da es unverhältnismäßig wäre, solche sensiblen Informationen weiter zu speichern.

32 Die EU-Institution sollte sorgfältig verfolgen, welche Maßnahmen das OLAF ergreift, sofern sich nach der Erstbewertung herausstellt, dass der Bericht an das OLAF zu übermitteln ist. Wenn das OLAF eine Untersuchung einleitet, muss die EU-Institution die Informationen nicht über einen längeren Zeitraum aufbewahren. Sofern das OLAF beschließt, keine Untersuchung einzuleiten, sollten die Informationen unverzüglich gelöscht werden.

33 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.

[18] Artikel 9 der Verordnung.
[19] Artikel 4 Absatz 1 Buchstabe e der Verordnung.
[20] Artikel 17 der Richtlinie, letzter Satz.
[21] Artikel-29-Datenschutzgruppe, Stellungnahme 1/2006, WP 117, S. 12

***Beispiel 8:*** *Eine EU-Institution 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 auf den Fall 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

34 Die EU-Institution (oder der für die Verarbeitung von Daten Verantwortliche, d. h. die Einrichtung, welche die Verarbeitungszwecke und -mittel für die Verarbeitung personenbezogener Daten festlegt) sollte geeignete technische und organisatorische Maßnahmen einrichten, um ein Schutzniveau zu gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu verarbeitenden personenbezogenen Daten angemessen ist[22]. Vertraulichkeit ist eine klare gesetzliche Pflicht und ein wichtiger Faktor, um die Bediensteten zur Meldung möglicher Bedenken zu ermutigen. Des Weiteren muss bei Sicherheitsmaßnahmen der Sensibilität der verarbeiteten personenbezogenen Daten Rechnung getragen werden. Vor diesem Hintergrund ist es wesentlich, geeignete Sicherheitsmaßnahmen einzurichten, um den Zugang von unbefugten Personen zu personenbezogenen Daten wirksam zu verhindern und ihre Integrität sicherzustellen.

35 **Die Notwendigkeit dieser Sicherheitsmaßnahmen muss unter Berücksichtigung der mit dem Verfahren zur Meldung von Missständen verbundenen Risiken durch ein manuelles oder automatisiertes Verfahren zur Risikobewertung der Informationssicherheit analysiert werden.** Nachdem die mit den betreffenden personenbezogenen Daten 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 Realisierbarkeit zu ergreifen sind. Da sich die Risiken im Laufe der Zeit verändern, muss die EU-Institution ihre Untersuchung, die Auswahl der Sicherheitsmaßnahmen und ihre Wirksamkeit regelmäßig überprüfen.

36 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 (zu aktualisieren).

***Beispiel 9:*** *Von besonderer Bedeutung für Vorgänge in Zusammenhang mit der Meldung von Missständen:*

[22] Artikel 33 der Verordnung.

*a) Der Zugang von Bediensteten zu personenbezogenen Daten muss strikt auf dem Grundsatz des berechtigten Informationsinteresses („Need-to-know") beruhen. Bedienstete, die Zugang zu diesen Informationen haben, müssen einer verstärkten Geheimhaltungspflicht unterliegen und der Zugang zu Berichten über die Meldung von Missständen muss überwacht werden, sei es in elektronischer Form oder in Papierform.*
*b) In technischer Hinsicht müssen die 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.*
*c) Aufgrund der hohen Vertraulichkeitsanforderungen betreffend diese Informationen ist besonders eine Verschlüsselung in Erwägung zu ziehen. Unbeschadet der Anwendung einer Verschlüsselung müssen Schutzmechanismen eingerichtet werden, mit denen der Zugang zu den Informationen bei Bedarf ermöglicht wird (gemeinsame Schlüssel, Aufzeichnung und sichere Verwahrung von Kennwörtern …).*

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

37 Rechenschaftspflicht bedeutet, dass EU-Institutionen ihren Datenschutzverpflichtungen nachzukommen haben und auch **in der Lage sein müssen, dies nachzuweisen**. (Artikel 4 Absatz 2 und Artikel 26 der Verordnung).

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

39 Jede EU-Institution, die personenbezogene Daten erhebt, verwendet und speichert (gemeinsam bezeichnet als „Verarbeitung"), ist dafür verantwortlich, dass die Datenschutzvorschriften eingehalten werden, und muss über diese Einhaltung Rechenschaft ablegen.

40 Generell müssen die EU-Institutionen 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 und auf Datenschutz besteht auch am Arbeitsplatz und die Menschen müssen über das Verfahren informiert werden. EU-Institutionen können nicht einfach davon ausgehen, dass die Mitarbeiter Bescheid wissen (Artikel 14 der Verordnung).

41 Am einfachsten kann eine EU-Institution ihrer Rechenschaftspflicht nachkommen, wenn sie die Datenschutzimplikationen neuer Prozesse schon bei deren Entwurf berücksichtigt (**Datenschutz durch Technikgestaltung – eingebauter Datenschutz**, Artikel 27 der Verordnung). Unterschiedliche Verarbeitungsvorgänge und unterschiedliche Technologien erfordern unterschiedliche Schutzmaßnahmen. Durch eine Einbeziehung ihres Datenschutzbeauftragten (DSB) schon in die frühen Phasen des Prozesses kann wertvolle Beratung und Orientierung eingeholt werden.

42 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 in dem jeweiligen Kontext für die vorgebrachten Vorwürfe erforderlich?

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

e. **Unterrichtung jeder Gruppe von betroffenen Personen:** Wer ist von der Meldung des Missstands betroffen?

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

g. **Durchführung einer Risikobewertung der Informationssicherheit:** Welchen potenziellen Sicherheitsrisiken können personenbezogene Daten in Fällen einer Meldung von Missständen ausgesetzt sein und wie minimieren Sie diese Risiken?

43 Zum Nachweis, dass Sie Ihrer Rechenschaftspflicht nachkommen, muss das Verfahren und seine Umsetzung dokumentiert werden. Folgende Dokumente sind erforderlich:

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

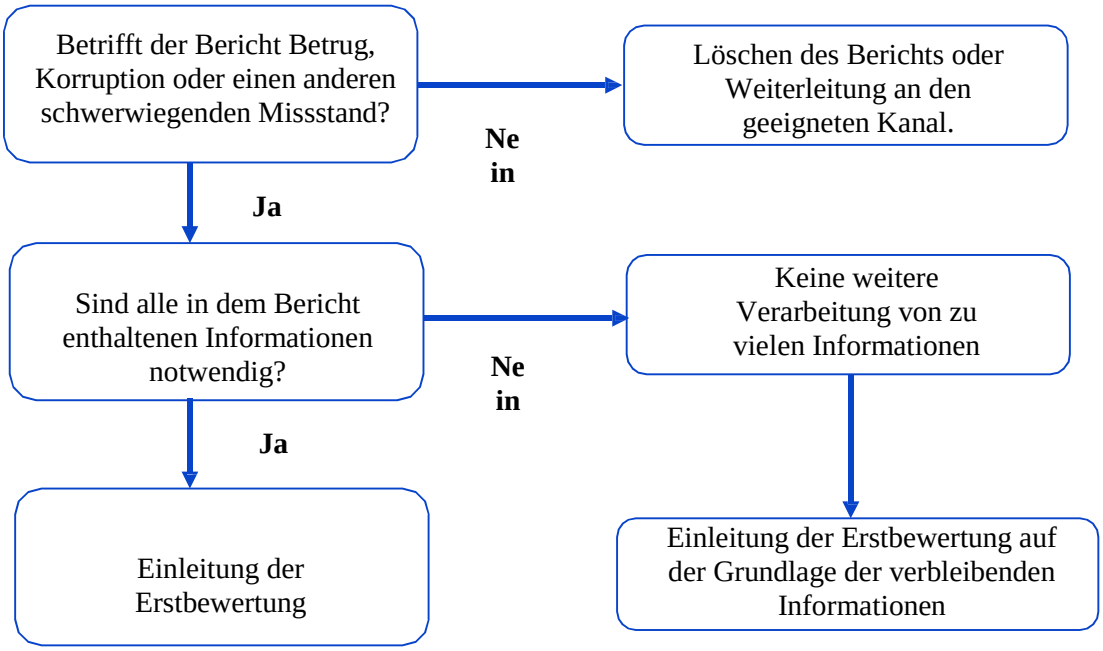
b. **Beschränkung bestimmter Rechte der betroffenen Personen** (die in den internen Vorschriften der EU-Institution enthalten sind), die Gründe, auf denen die Beschränkungen basieren, sowie die Begründung für die Anwendung der Beschränkungen;

c. ein **Aufschub bei der Erteilung von Informationen** für die betreffende Person (im Einklang mit den internen Vorschriften);

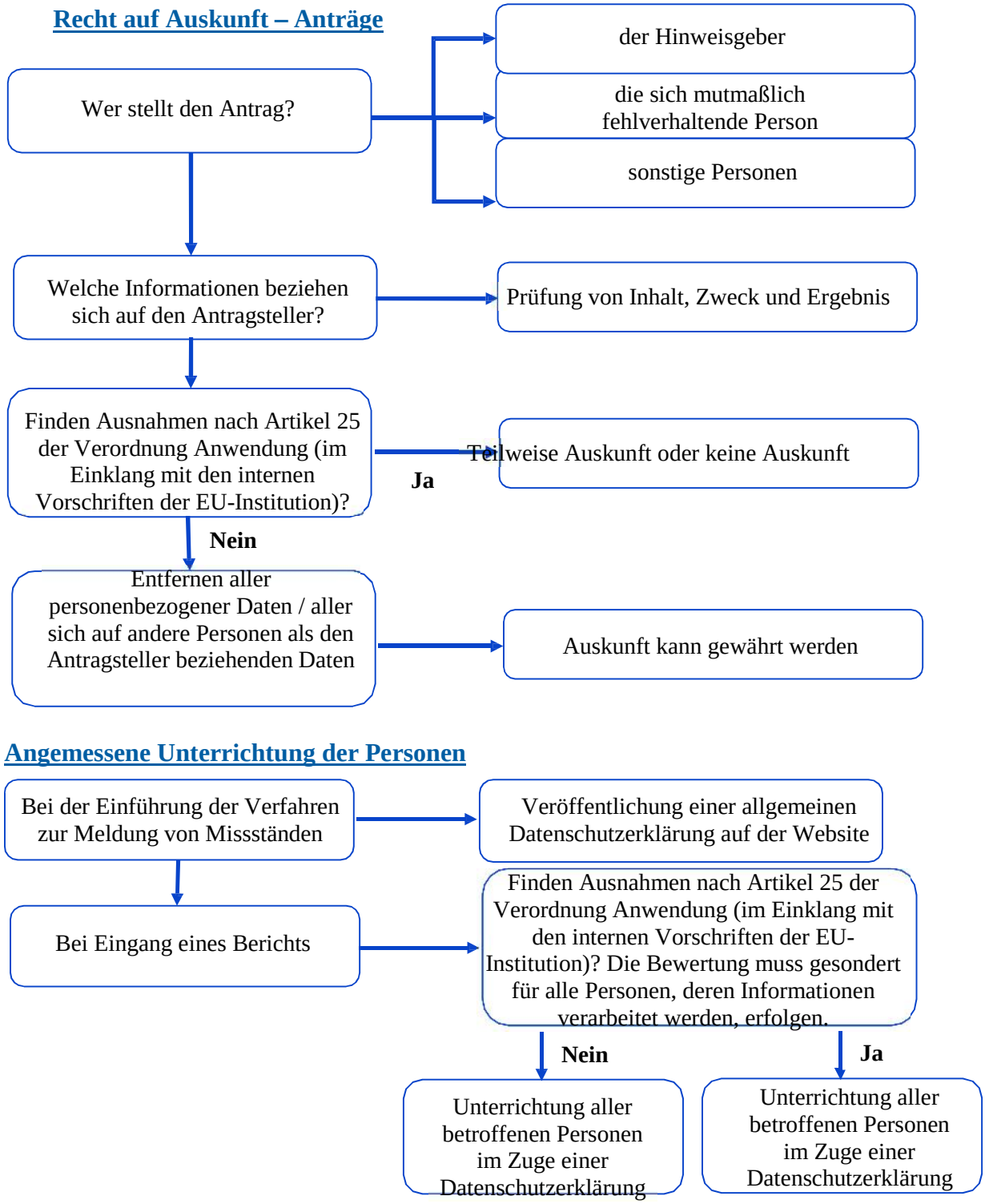
d. die für dieses konkrete Verfahren vorgenommene **Risikobewertung**.

## 12. FLUSSDIAGRAMME – VERFAHREN ZUR MELDUNG VON MISSSTÄNDEN

## 12.1 Umgang mit Berichten über die Meldung von Missständen



## 12.2 Sicherstellung der Rechte von Personen



## WEITERFÜHRENDE LITERATUR

Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden

### Beispiele für Stellungnahmen des EDSB

Fall Nr. 2016-1083 – Stellungnahme zur den internen Verfahren und Leitlinien zu Whistleblowing bei der EMCDDA

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)

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