Die EU-Datenschutzgrundverordnung

Enormer Nachholbedarf bei der Umsetzung und erste Erfahrungen

"Im Regen" von Peter Strunk

Seit 25. Mai 2018 ist die EU-Datenschutzgrundverordnung (DSGVO) in Kraft. Betroffen sind alle, die personenbezogene Daten verarbeiten, wozu auch Telefonnummern und E-Mails gehören, so dass faktisch jedes Unternehmen, jeder Selbständige und jeder Verein betroffen ist. Bei Datenschutzverstößen drohen Bußgelder von den Datenschutzbehörden in Höhe von bis zu 4 Prozent des weltweiten Jahresumsatzes oder von bis zu 20 Millionen €.

Noch immer haben viele Unternehmen, Selbständige und Vereine die neuen Datenschutzregeln nicht (vollständig) umgesetzt. Manche Unternehmen haben noch nicht einmal eine Datenschutzerklärung auf ihrer Homepage oder verwenden nicht die erforderliche https://-Verschlüsselung, was einerseits von Mitbewerbern und Abmahnvereinen kostenpflichtig abgemahnt werden kann und andererseits von den Datenschutzbehörden mit Bußgeldern belegt werden kann.

Die ersten kostenpflichtigen Abmahnungen wegen Datenschutzverstößen wurden bereits verschickt, z.B. wegen fehlender Information über die Verwendung der Schriften von Google Web Fonts in der Datenschutzerklärung der Unternehmenshomepage. Erpresserschreiben, deren Spuren von der Kriminalpolizei in die USA zurückverfolgt werden konnten, wurden versandt mit der Drohung, die Kunden des Empfängers und die Datenschutzbehörden von Sicherheitslücken im Online-Shop des Empfängers zu informieren, falls der geforderte Geldbetrag in Höhe von 1.500 € nicht gezahlt werden würde. Die angehängten Screenshots hatten tatsächlich Auszüge aus der Kundenliste abgebildet.

Des Weiteren versendet ein angeblicher Tim F. (Name wurde aus Datenschutzgründen gekürzt) völlig anlasslos datenschutzrechtliche Auskunftsersuchen mit Fristsetzungen an zahlreiche Unternehmen, denen er völlig unbekannt ist. Es ist zu befürchten, dass hier die nächste Abmahnwelle vorbereitet werden soll, die alle diejenigen treffen soll, die nicht fristgerecht und rechtskonform Auskunft erteilen.

Was ist konkret zu tun? Hier eine kurze Checkliste für Eilige - ohne Anspruch auf Vollständigkeit:

1. Datenschutzerklärung, insbesondere auf der eigenen Webseite, ergänzen

Kommerzielle Webseiten benötigen - wie bisher - eine Datenschutzerklärung. Aufgrund der neuen DSGVO ist nunmehr auch über die zu Grunde gelegten Rechtsgrundlagen zu informieren und die teilweise neuen Rechte der Betroffenen, z.B. das Recht auf Datenübertragbarkeit und das Recht auf Beschwerde bei der Datenschutzaufsicht. Darüber hinaus müssen viele der durch das Gesetz geforderten Informationen für jede Funktion der Webseite gesondert bewertet werden.

Da die Informationen gem. Art. 13 Abs. 1 DSGVO „bei Erhebung" der personenbezogenen Daten gegeben werden müssen, sollte die Datenschutzerklärung - wie bisher - regelmäßig mit nur einem Klick erreichbar sein. Dem kann durch die Aufnahme des Links im Header oder Footer neben dem Impressum nachgekommen werden.

Die betroffenen Personen, z.B. die Besucher einer Webseite, müssen umfangreicher als bisher darüber informiert werden, wer, wie, wann und wo ihre Daten speichert und welche Rechte sie diesbezüglich haben. Da-

her muss eine bestehende Datenschutzerklärung auf der Webseite entsprechend ergänzt bzw. neu gestaltet werden. Die erforderlichen Informationen müssen präzise, transparent, verständlich und leicht zugänglich sein.

Eine rechtskonforme Datenschutzerklärung muss den Betroffenen folgende Informationen zur Verfügung stellen:

- Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls das nicht möglich ist, die Kriterien für die Festlegung dieser Dauer

- Belehrung darüber, dass der Betroffene folgende Rechte bezüglich seiner Daten hat: Auskunftsrecht, Recht auf Berichtigung oder Löschung, Recht auf Einschränkung der Verarbeitung, Widerspruchsrecht gegen die Verarbeitung, Recht auf Datenübertragbarkeit

- falls die Datenverarbeitung auf einer Einwilligung des Betroffenen, zum Beispiel Kunden, beruht, muss ein gesonderter Hinweis darauf erfolgen, dass die Einwilligung jederzeit widerrufen werden kann und die Datenverarbeitung bis zum Zeitpunkt des Widerrufs rechtmäßig bleibt

- Aufklärung über das Beschwerderecht bei der Aufsichtsbehörde

- Information darüber, ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist und ob die betreffende Person verpflichtet ist, die Daten bereitzustellen und welche Folgen eine Weigerung hätte

- falls eine automatisierte Entscheidung im Einzelfall getroffen werden soll oder eine andere Profiling-Maßnahme stattfinden soll, muss der Betroffene über deren Tragweite, Logik und Algorithmus informiert werden

- wer einen Datenschutzbeauftragten hat, muss diesen mit seinen Kontaktdaten auf seiner Homepage benennen

Zusätzlich müssen die betroffenen Personen, z.B. Kunden, Vertragspartner, Vereinsmitglieder etc., über die weitere Datenverarbeitung informiert werden, z.B. durch ein Rundschreiben.

2. Auftragverarbeitungsverträge abschließen

Fast jedes Unternehmen hat einen externen IT-Dienstleister, dem Einblick in die eigene Datenhaltung mit personenbezogenen Daten gewährt wird und der daher "Auftragsverarbeiteter" im Sinne der Datenschutzgrundverordnung ist. Wer einen externen IT-Dienstleister/Auftragsverarbeiter einschalten möchte, muss vorher prüfen, ob dieser datenschutzkonform arbeitet. Mit dem externen IT-Dienstleister/Auftragsverarbeiter muss ein schriftlicher Vertrag abgeschlossen werden, mit dem sich der Auftraggeber umfassende Kontrollrechte einräumen lassen muss.

3. Für IT-Sicherheit sorgen

Beispielsweise muss jeder, der auf seiner Webseite ein Kontaktformular anbietet, https:// als Transportverschlüsselung verwenden. Wer mobile Geräte, wie z.B. Smartphones, Tablets oder Notebooks, verwendet, auf denen personenbezogene Daten gespeichert sind, muss diese neben dem Kennwort zum Entsperren des Nutzer-Accounts auch mit einer Datenträgerverschlüsselung ausstatten. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt hierfür z.B. das kostenfreie Produkt VeraCrypt, s. https://veracrypt.codeplex.com. Bei der Verwendung von Cloud-Diensten sollten personenbezogene Daten vor dem Versenden verschlüsselt werden, so dass der Cloud-Anbieter keine Zugriffsmöglichkeit auf diese Daten hat. Die regelmäßige Durchführung von Back-ups zur Abwehr von Schadsoftware ist Pflicht. Unter dem Link https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Ueberblick-IT-Grundschutz.pdf?__blob=publicationFile&v=4 stellt das BSI einen Überblick über die Anforderungen an einen IT-Grundschutz als Entscheidungshilfe zur Verfügung.

4. Verzeichnis von Verarbeitungstätigkeiten erstellen

Jeder, der personenbezogene Daten verarbeitet oder speichert, muss ein Verzeichnis von Verarbeitungstätigkeiten erstellen, in dem Folgendes dokumentiert werden muss.

- Name und die Kontaktdaten des Verantwortlichen, ggfs. auch Vertreter und Datenschutzbeauftragte

- Zwecke der Verarbeitung

- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten

- Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen

- gegebenenfalls Übermittlungen von personenbezogenen Daten in ein Drittland oder an eine internationale Organisation

- wenn möglich, vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien

- wenn möglich, allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (TOM)

Verschiedene Datenschutzbehörden, wie z.B. das Bayerisches Landesamt für Datenschutzaufsicht, stellen auf ihren Webseiten Musterverzeichnisse für Verarbeitungstätigkeiten für verschiedene Branchen zur Verfügung: https://www.lda.bayern.de/de/kleine-unternehmen.html.

Natürlich muss bei der Erstellung des Verfahrensverzeichnisses auch geprüft werden, ob die dokumentierte Datenverarbeitung rechtmäßig erfolgt. Das Verzeichnis muss stets aktuell sein und ist auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen.

5. Datenschutzbeauftragten benennen

Wer in seinem Unternehmen oder Verein mindestens 10 Personen damit beschäftigt, personenbezogene Daten automatisiert zu verarbeiten, muss einen internen oder externen Datenschutzbeauftragten benennen. Das Gleiche gilt für Unternehmen oder Vereine, die im Rahmen einer Kerntätigkeit besonders sensible Daten verarbeiten, zum Beispiel Gesundheitsdaten. Die Benennung sollte aus Beweisgründen schriftlich erfolgen. Die Kontaktdaten des Datenschutzbeauftragten müssen auf der Homepage genannt und der zuständigen Aufsichtsbehörde mitgeteilt werden.

6. Betriebsvereinbarung anpassen oder ergänzen

Wer einen Betriebsrat hat, sollte prüfen, ob die bestehenden Betriebsvereinbarungen (auch) Datenverarbeitungsvorgänge regeln, zum Beispiel Vereinbarungen betreffend bring your own device (BYOD) enthalten. Wenn dies der Fall ist, müsste geprüft werden, ob die bestehenden Regelungen den Vorgaben der EU-Datenschutzgrundverordnung entsprechen. Möglicherweise ist es sinnvoll, eine Rahmen-Betriebsvereinbarung abzuschließen, zum Beispiel hinsichtlich der allgemeinen Informationspflichten des Arbeitgebers. Das ist wichtig, weil anderenfalls auch Beweisverwertungsverbote drohen: Datenerhebungen, die nicht im Einklang mit der EU-Datenschutzgrundverordnung stehen, können in Kündigungsschutzverfahren möglicherweise nicht zur Rechtfertigung von Kündigungen angeführt werden.

7. Datenschutz-Folgeabschätzung vornehmen

Für besonders risikobehaftete Datenverarbeitungen muss mittels einer Risikoanalyse festgestellt werden, ob eine sogenannte Datenschutz-Folgenabschätzung (DSFA) durchzuführen ist, z.B. in folgenden Fällen:

- bei systematischer und umfassender Bewertung persönlicher Aspekte von Personen auf Grundlage automatisierter Datenverarbeitung, einschließlich Profiling
- bei umfangreicher Verarbeitung sensibler Daten, zum Beispiel politischer Meinungen, religiöser oder weltanschaulicher Überzeugungen und Daten über Straftaten
- bei systematischer weiträumiger Überwachung öffentlich zugänglicher Bereiche

Auf Aufforderung einer Aufsichtsbehörde müssen Datenverantwortliche nachweisen können, dass sie alle Datenschutzregeln einhalten.

8. Krisenreaktionsplan für Datenschutzvorfälle erstellen

Da im Falle einer Datenschutzverletzung schnell gehandelt werden muss, sollte für diesen Fall ein Krisenreaktionsplan erstellt werden. Es sollten interne Richtlinien formuliert werden, wie im Fall einer Datenpanne zu verfahren ist und wer zuständig ist. Sämtliche Mitarbeiter sollten hierüber unterrichtet werden. Die Aufsichtsbehörde sollte innerhalb von 72 Stunden ab Kenntnis von der Datenpanne informiert werden. Gegebenenfalls sollte auch Strafanzeige bei den Strafverfolgungsbehörden erstattet werden. Darüber hinaus sollten auch die

Grundsätze des Datenschutzes nach Art. 5 DSGVO

Der Verantwortlich ist für die Einhaltung der nachfolgenden Grundsätze verantwortlich und muss deren Einhaltung nachweisen können, sog. Rechenschaftspflicht:

1. Rechtmäßigkeit: Ist ein Erlaubnistatbestand vorhanden?

Ist die Verarbeitung rechtmäßig, nach Treu und Glauben und für die betroffene Person nachvollziehbar, vgl. Art. 6 Abs. 1 Buchst. a - f DS GVO?

2. Zweckbindungsgrundsatz

Wurde der Zweck deutlich, konkret und detailliert vereinbart? Falls die Verarbeitung zu anderem Zweck erfolgt: Ist der neue Zweck mit dem altem Zweck vereinbar?

3. Datenminimierung

Sind die Daten für den Zweck angemessen und erheblich sowie auf das für die Zwecke notwendige Maß beschränkt? Sind Strategien und Maßnahmen zur Datenminimierung getroffen, z.B. Pseudonymisierung und technische Vorrichtungen?

4. Datenrichtigkeit

Sind die verarbeiteten Daten richtig und auf dem neuesten Stand? Wurden Maßnahmen getroffen, um zu gewährleisten, dass personenbezogene Daten, die hinsichtlich des Zwecks ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden? Gibt es eine Dienstvereinbarung, die Regelungen zu solchen Korrekturprozessen enthält?

5. Speicherbegrenzung

Sind klare Regelungen zu Speicherdauer, sog. Löschkonzept, von personenbezogenen Daten in den Unternehmensrichtlinien festgelegt und in der Dienstvereinbarung getroffen?

6. Integrität und Vertraulichkeit

Sind technisch-organisatorischen Maßnahmen vorhanden, um den Schutz vor unbefugter, unrechtmäßiger Verarbeitung sowie vor Schädigung, Zerstörung oder Verlust zu gewährleisten? Ist die Verarbeitung besonderer Datenkategorien, z. B. Religionszugehörigkeit, Gesundheitsdaten, biometrische Daten, ausreichend gesichert?

von der Datenschutzverletzungen betroffenen Personen zeitnah von der Datenpanne unterrichtet werden (soweit damit die strafrechtlichen Ermittlungen nicht gefährdet werden oder dadurch neue Sicherheitsrisiken entstehen können.).

9. Fazit

Obwohl einige Einzelfragen in Bezug auf die Umsetzung der EU-Datenschutzgrundverordnung immer noch nicht abschließend geklärt sind, sollte jedes Unternehmen, jeder Selbständige und jeder Verein, der personenbezogene Daten verarbeitet, dafür Sorge tragen, dass er - falls noch nicht geschehen - schnellstmöglich alle Anforderung der DSGVO erfüllt.

Gabriele Freifrau von Thüngen-Reichenbach

Links (Auswahl):

- https://www.lda.bayern.de/de/datenschutz_eu.html
- https://www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/index.html

Literaturtipp:

Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine - Das Sofortmaßnahmen-Paket, herausgegeben vom Bayerischen Landesamt für Datenschutzaufsicht, C. H. Beck Verlag, 5,50 €

Rechtsanwältin **Gabriele Freifrau von Thüngen-Reichenbach** ist Fachanwältin für gewerblichen Rechtsschutz, für Urheber- und Medienrecht und für IT-Recht in Coburg/Bayern. Darüber hinaus ist sie zertifizierte Datenschutzbeauftragte - DSB TÜV-Süd. Sie hat sich auf die Beratung von Unternehmen und Selbständigen spezialisiert. Sie berät ihre Mandanten bei der Vertragsgestaltung, der rechtskonformen Gestaltung ihrer Webseiten, der Entwicklung und Umsetzung umfassender Schutzrechts-Strategien für geistiges Eigentum (Marken und Designs), und der Umsetzung gesetzlicher Regelungen, z.B. Datenschutz und Wettbewerbsrecht, insbesondere in der digitalen Welt. www.von-thuengen.de

DSGVO FAQ

Was sind personenbezogene Daten?

Gemäß Artikel 4 Abs. 1 EU-DSGVO sind personenbezogene Daten im Sinne dieser Verordnung alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen.

Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Personenbezogene Daten sind beispielsweise:

- Name, Alter, Familienstand, Geburtsdatum
- Anschrift, Telefonnummer, E-Mail-Adresse
- Fotos, Videoaufnahmen, Röntgenbilder, Tonbandaufnahmen
- Konto-, Kreditkartennummer
- Kraftfahrzeugnummer, Kfz-Kennzeichen
- Personalausweisnummer, Sozialversicherungsnummer
- Vorstrafen
- genetische Daten und Krankendaten
- Werturteile wie zum Beispiel Zeugnisse
- Mitgliedschaft in Vereinen

Kundendaten gehören ebenso zu den personenbezogenen Daten wie die Personaldaten von Beschäftigten.

Angaben über juristische Personen, wie zum Kapitalgesellschaften oder eingetragene Vereine, sind keine personenbezogenen Daten. Etwas anderes gilt dann, wenn sich die Angaben auch auf die hinter der juristischen Person stehende/n natürliche/n Person/en beziehen, d.h. auf sie „durchschlagen“. Dies kann beispielsweise bei einer Ein-Personen-GmbH der Fall sein, da in diesem Fall enge finanzielle, persönliche oder wirtschaftliche Verflechtungen zwischen der natürlichen und der juristischen Person bestehen.

Was versteht man unter Verarbeitung im Sinne der DSGVO ?

Gemäß Art. 4 Nr. 2 DSGVO ist „Verarbeitung“ jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Wichtig: Bereits das bloße Speichern, d.h. zum Beispiel beim Empfang eines Email-Schreibens oder einer SMS, ist Verarbeitung im Sinne der DSGVO.

Bei welcher Art von Verarbeitung gilt die DSGVO ?

Gemäß Art. 2 DSGVO gilt die DSGVO für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Dateisystem ist jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird (Art. 4 Nr. 6 DSGVO).

Grundsätzlich fallen also körperlich, d.h. auf Papier geführte Akten oder Aktensammlungen sowie ihre Deckblätter bzw. dort gespeicherte personenbezogene Daten nicht in den Anwendungsbereich der DSGVO. Etwas anderes gilt allerdings, wenn die Akte dateimäßig strukturiert ist, also aufgrund einer vorgegebenen Struktur nach bestimmten Kriterien auswertbar ist.

Notizen, die als Gedächtnisstütze gemacht wurden und alsbald wieder vernichtet werden, fallen ebenfalls nicht in den Anwendungsbereich der DSGVO.

Wann ist die Verarbeitung personenbezogener Daten rechtmäßig?

Gemäß Art. 6 Abs. 1 DSGVO ist die Verarbeitung nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

- Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
- die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
- die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Welche Rechte hat der Betroffene ?

- das Recht, eine einmal erteilte Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen, Art. 7 Abs. 3 DSGVO
- das Recht, Auskunft über seine verarbeiteten personenbezogenen Daten zu verlangen, Art. 15 DSGVO
- das Recht, unverzüglich die Berichtigung unrichtiger oder Vervollständigung seiner gespeicherten personenbezogenen Daten zu verlangen, Art. 16 DSGVO
- das Recht, die Löschung seiner gespeicherten personenbezogenen Daten zu verlangen, soweit nicht die Verarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung und Information, zur Erfüllung einer rechtlichen Verpflichtung, aus Gründen des öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist, Art. 17 DSGVO
- das Recht, die Einschränkung der Verarbeitung seiner personenbezogenen Daten zu verlangen, soweit die Richtigkeit der Daten von ihm bestritten wird, die Verarbeitung unrechtmäßig ist, er aber deren Löschung ablehnt und der Verarbeiter die Daten nicht mehr benötigt, der Betroffene jedoch diese zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt oder er gemäß Art. 21 DSGVO Widerspruch gegen die Verarbeitung eingelegt hat, Art. 18 DSGVO
- das Recht, seine personenbezogenen Daten, die er bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesebaren Format zu erhalten oder die Übermittlung an einen anderen Verantwortlichen zu verlangen, Art. 20 DSGVO
- das Recht, Widerspruch gegen die Verarbeitung seiner personenbezogenen Daten einzulegen, sofern seine personenbezogenen Daten auf Grundlage von berechtigten Interessen gemäß Art. 6 Abs. 1 S. 1 lit. f DSGVO verarbeitet werden, soweit dafür Gründe vorliegen, die sich aus Ihrer besonderen Situation ergeben oder sich der Widerspruch gegen Direktwerbung richtet, Art. 21 DSGVO
- das Recht, sich bei einer Aufsichtsbehörde zu beschweren, Art. 77 DSGVO

Welche Aufsichtsbehörde ist zuständig für eine Beschwerde ?

Die Person, die sich beschweren möchte, hat die Wahl zwischen verschiedenen zuständigen Aufsichtsbehörden:

- die Aufsichtsbehörde in dem Mitgliedstaat ihres gewöhnlichen Aufenthaltsorts
- die Aufsichtsbehörde in dem Mitgliedstaat ihres Arbeitsplatzes oder
- die Aufsichtsbehörde des Orts des mutmaßlichen Verstoßes

Eine Liste der Aufsichtsbehörden mit den jeweiligen Kontaktdaten finden Sie unter folgendem Link:

https://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html