EMPFEHLUNGEN

EMPFEHLUNG DER KOMMISSION

vom 1. März 2011

Leitlinien für die Anwendung der Datenschutzbestimmungen im System zur Zusammenarbeit im Verbraucherschutz (CPCS)

(2011/136/EU)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 292,

in Erwägung nachstehender Gründe:

(1) Mit der Verordnung (EG) Nr. 2006/2004 des Europäischen Parlaments und des Rates vom 27. Oktober 2004 über die Zusammenarbeit zwischen den für die Durchsetzung der Verbraucherschutzgesetze zuständigen nationalen Behörden (Verordnung über die Zusammenarbeit im Verbraucherschutz) [1] (im Folgenden „Verordnung über die Zusammenarbeit") wird eine bessere Zusammenarbeit bei der Durchsetzung der Verbraucherschutzvorschriften im Binnenmarkt angestrebt, wird ein EU-weites Netz für die Zusammenarbeit der nationalen Durchsetzungsbehörden (im Folgenden „Netz") geschaffen und werden der Rahmen und die allgemeinen Bedingungen festgelegt, in dem bzw. unter denen die Durchsetzungsbehörden der Mitgliedstaaten zusammenarbeiten sollen, um die kollektiven wirtschaftlichen Interessen der Verbraucher zu schützen.

(2) Die Zusammenarbeit der nationalen Durchsetzungsbehörden ist von zentraler Bedeutung dafür, dass der Binnenmarkt gut funktioniert; dank dieses Netzes kann jede Behörde andere Behörden um Hilfe bei der Untersuchung möglicher Verstöße gegen die Verbraucherschutzvorschriften der EU ersuchen.

(3) Ziel des Systems zur Zusammenarbeit im Verbraucherschutz (im Folgenden „CPCS" nach englisch *Consumer Protection Cooperation System*) ist es, die Durchsetzungsbehörden in die Lage zu versetzen, in einer sicheren Umgebung Informationen über mögliche Verstöße gegen die Verbraucherschutzvorschriften auszutauschen.

(4) Der elektronische Informationsaustausch zwischen den Mitgliedstaaten muss den Bestimmungen für den Schutz personenbezogener Daten in der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr [2] (im Folgenden „Datenschutzrichtlinie") und in der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr [3] (im Folgenden „Datenschutzverordnung") genügen.

(5) Das Recht auf Datenschutz wird in Artikel 8 der Charta der Grundrechte der Europäischen Union anerkannt. Das CPCS sollte gewährleisten, dass die verschiedenen Verpflichtungen und Zuständigkeiten im Hinblick auf die Datenschutzbestimmungen, die sich die Kommission und die Mitgliedstaaten teilen, klar sind und dass die von der Erfassung ihrer Daten betroffenen Personen (im Folgenden „betroffene Personen") Informationen und leichten Zugang zu Verfahren zur Wahrnehmung ihrer Rechte erhalten.

(6) Es ist angebracht, Leitlinien für die Anwendung der Datenschutzbestimmungen im Rahmen des CPCS (im Folgenden „Leitlinien") aufzustellen, damit die Datenschutzbestimmungen bei der Verarbeitung von Daten im Rahmen des CPCS eingehalten werden.

(7) Die Durchsetzungsbeamten sollten angehalten werden, ihre nationalen Datenschutz-Aufsichtsbehörden um Orientierung und Hilfe dazu zu ersuchen, wie sich diese Leitlinien am besten im Einklang mit den nationalen Vorschriften anwenden lassen, und bei Bedarf zu gewährleisten, dass bei Datenverarbeitungsvorgängen im CPCS auf nationaler Ebene die entsprechenden Melde- und Vorabprüfverfahren durchgeführt werden.

(8) Zur Teilnahme an den Schulungen, die die Kommission organisieren wird, um die Anwendung der Leitlinien zu unterstützen, sollte kräftig ermuntert werden.

(9) Eine Rückmeldung an die Kommission zur Anwendung der Leitlinien sollte spätestens zwei Jahre nach Annahme dieser Empfehlung erfolgen. Die Kommission sollte dann eine erneute Bewertung des Datenschutzniveaus in Bezug auf das CPCS vornehmen und prüfen, ob weitere Maßnahmen, auch in Form von Vorschriften, erforderlich sind.

[1] ABl. L 364 vom 9.12.2004, S. 1.

[2] ABl. L 281 vom 23.11.1995, S. 31.

[3] ABl. L 8 vom 12.1.2001, S. 1.

(10) Es sollte das Nötige veranlasst werden, um den Akteuren und Nutzern des CPCS die Anwendung der Leitlinien zu erleichtern. Die nationalen Datenschutzbehörden und der Europäische Datenschutzbeauftragte sollten die Entwicklungen und die Anwendung der Datenschutzvorkehrungen im Zusammenhang mit dem CPCS aufmerksam beobachten.

(11) Die Leitlinien ergänzen die Entscheidung 2007/76/EG der Kommission [1] und berücksichtigen die Stellungnahme der gemäß Artikel 29 der Datenschutzrichtlinie eingesetzten Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten [2] und die Stellungnahme des gemäß Artikel 41 der Datenschutzverordnung eingesetzten Europäischen Datenschutzbeauftragten [3] (im Folgenden „EDSB“) —

HAT FOLGENDE EMPFEHLUNG ABGEGEBEN:

Die Mitgliedstaaten sollten die Leitlinien im Anhang befolgen.

Brüssel, den 1. März 2011

Für die Kommission
John DALLI
Mitglied der Kommission

[1] ABl. L 32 vom 6.2.2007, S. 192.
[2] Stellungnahme 6/2007 zu Datenschutzfragen im Zusammenhang mit dem Kooperationssystem für Verbraucherschutz (CPCS) 01910/2007/DE, WP 130, angenommen am 21. September 2007.
[3] EDSB-Stellungnahme 2010-0692.

ANHANG

Leitlinien für die Anwendung der Datenschutzbestimmungen im Rahmen des Systems zur Zusammenarbeit im Verbraucherschutz (CPCS)

1. EINLEITUNG

Die Zusammenarbeit der nationalen Verbraucherschutzbehörden ist unentbehrlich für das reibungslose Funktionieren des Binnenmarkts: Ohne wirksame Durchsetzung von Rechten und Ansprüchen über die Landesgrenzen hinweg zögern Verbraucher, Angebote aus dem Ausland anzunehmen, und schwindet das Vertrauen in den Binnenmarkt; außerdem kommt es zu Wettbewerbsverzerrungen.

Das CPCS ist eine IT-Anwendung, die gemäß der Verordnung über die Zusammenarbeit geschaffen wurde und einen strukturierten Rahmen für den Informationsaustausch zwischen den nationalen Verbraucherschutzbehörden vorgibt, die dem Netz angeschlossen sind. Es ermöglicht einer Behörde, andere dem Netz angeschlossene Behörden um Hilfe zu ersuchen bei der Untersuchung möglicher Verstöße gegen das EU-Verbraucherschutzrecht, beim Vorgehen gegen diese Verstöße sowie bei der Durchsetzung von Maßnahmen zur Unterbindung illegaler Geschäftspraktiken von Verkäufern und Dienstleistungserbringern, wenn in anderen EU-Ländern lebende Verbraucher davon betroffen sind. Informationsersuchen und die sonstige Kommunikation zwischen den zuständigen Behörden betreffend die Durchsetzung der Verordnung über die Zusammenarbeit erfolgen über das CPCS.

Zweck der Verordnung über die Zusammenarbeit ist eine bessere Durchsetzung der Verbraucherschutzvorschriften im Binnenmarkt, wozu ein EU-weites Netz nationaler Durchsetzungsbehörden aufgebaut worden ist, und die Regelung der Zusammenarbeit der Mitgliedstaaten. In der Verordnung über die Zusammenarbeit ist festgelegt, dass der Informationsaustausch und die Amtshilfeersuchen der nationalen Durchsetzungsbehörden über eine eigene Datenbank erfolgen müssen. Das CPCS wurde daher so konzipiert, dass die administrative Zusammenarbeit und der Informationsaustausch im Hinblick auf die Durchsetzung der EU-Verbraucherschutzvorschriften problemlos erfolgen können.

Die Zusammenarbeit ist auf innergemeinschaftliche Verstöße gegen die Rechtsvorschriften beschränkt, die im Anhang der Verordnung über die Zusammenarbeit aufgeführt sind, welche die kollektiven wirtschaftlichen Interessen der Verbraucher schützt.

2. ANWENDUNGSBEREICH UND ZWECK DIESER LEITLINIEN

Die Leitlinien sind die Antwort auf das zentrale Anliegen, ein Gleichgewicht zwischen einer effizienten und effektiven Zusammenarbeit der zuständigen Behörden der Mitgliedstaaten einerseits und der Achtung grundlegender Rechte im Zusammenhang mit dem Schutz von Privatsphäre und personenbezogenen Daten andererseits zu finden.

Personenbezogene Daten sind gemäß der Datenschutzrichtlinie [1] alle Informationen über eine bestimmte oder bestimmbare natürliche Person; als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

Da die nationalen Durchsetzungsbeamten (Sachbearbeiter), die das CPCS nutzen, möglicherweise nicht immer Datenschutzexperten sind und möglicherweise die eigenen nationalen Datenschutzvorschriften nicht immer gut genug kennen, ist es ratsam, den CPCS-Nutzern Leitlinien anzubieten, in denen die Funktionsweise des CPCS aus einer praktischen Datenschutzperspektive erklärt wird und zugleich ausführlich die in das System eingebauten Sicherheitsvorkehrungen und die mit der Nutzung verbundenen potenziellen Risiken beschrieben werden.

Ziel der Leitlinien ist es, die wichtigsten Datenschutzfragen im Zusammenhang mit dem CPCS zu behandeln und eine nutzerfreundliche Anleitung zu bieten, in der sich alle CPCS-Nutzer zurechtfinden. Sie sind nicht als umfassende Abhandlung über die Datenschutzaspekte des CPCS gedacht.

Es wird sehr empfohlen, die Datenschutzbehörden in den Mitgliedstaaten zu konsultieren, um sicherzustellen, dass die Leitlinien um spezifische Verpflichtungen ergänzt werden, die in den nationalen Datenschutzgesetzen verankert sind. CPCS-Nutzer können von diesen nationalen Datenschutzbehörden auch weitere Hilfe und Anleitung erhalten, damit gewährleistet ist, dass die Datenschutzanforderungen eingehalten werden. Eine Liste dieser Behörden mit Kontaktdaten und Websites gibt es unter:

http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/#eu

Es sollte klar sein, dass die Verarbeitung personenbezogener Daten im Einklang mit den besonderen Grundsätzen und Bestimmungen der Datenschutzrichtlinie erfolgen muss. Die Sachbearbeiter sind im Zusammenhang mit der Verordnung über die Zusammenarbeit befugt, Daten (auch personenbezogene) über das CPCS auszutauschen, wenn der Zweck der Verarbeitung darin besteht, einen Verstoß gegen eine der im Anhang der Verordnung aufgeführten EU-Verbraucherschutzvorschriften zu beenden. Vor der Verarbeitung solcher Daten ist jedoch sorgfältig zu prüfen, ob die Datenschutzgrundsätze beachtet werden und ob die Verarbeitung der Daten für die Erreichung der Ziele der Verordnung über die Zusammenarbeit unbedingt erforderlich ist.

[1] Artikel 2 Buchstabe a.

Sachbearbeiter mit Zugang zum CPCS müssen folglich in jedem einzelnen Fall eine Bewertung vornehmen, bevor personenbezogene Daten verarbeitet werden dürfen [1]. Zweck dieser Leitlinien ist es, den Sachbearbeitern als Richtschnur einige Datenschutzgrundsätze an die Hand zu geben, die ihnen bei der Bewertung helfen sollen.

Außerdem sollen einige der komplexen Merkmale der CPCS-Architektur im Zusammenhang mit der gemeinsamen Verarbeitung und der gemeinsamen Kontrolle erläutert werden (welche Aufgaben haben die Kommission und die zuständigen Behörden der Mitgliedstaaten als „gemeinsame Kontrolleure" des CPCS-Datenaustauschs).

3. DAS CPCS — EINE IT-ANWENDUNG FÜR DIE ZUSAMMENARBEIT BEI DER DURCHSETZUNG

Das CPCS ist eine IT-Anwendung, entwickelt und verwaltet von der Kommission in Zusammenarbeit mit den Mitgliedstaaten. Zweck des CPCS ist es, die Mitgliedstaaten bei der praktischen Anwendung des EU-Verbraucherschutzrechts zu unterstützen. Genutzt wird es vom Netz, das aus den von den Mitgliedstaaten und den EWR-Ländern benannten Behörden besteht, die bei der Durchsetzung der Verbraucherschutzvorschriften gemäß der Verordnung über die Zusammenarbeit zusammenarbeiten und Informationen austauschen sollen.

In Artikel 10 der Verordnung über die Zusammenarbeit heißt es:

„Die Kommission unterhält eine elektronische Datenbank, in der sie alle ihr gemäß den Bestimmungen der Artikel 7, 8 und 9 zugehenden Informationen speichert und verarbeitet. Die Datenbank darf nur den zuständigen Behörden für Abfragen zur Verfügung gestellt werden."

Artikel 12 Absatz 3 der Verordnung lautet:

„Amtshilfeersuchen und jegliche Übermittlung von Informationen erfolgen schriftlich unter Verwendung eines Standardformulars und werden auf elektronischem Wege über die in Artikel 10 vorgesehene Datenbank übermittelt."

Das CPCS erleichtert die Zusammenarbeit und den Informationsaustausch ausschließlich betreffend innergemeinschaftliche Verstöße gegen die im Anhang der Verordnung über die Zusammenarbeit aufgeführten Richtlinien und Verordnungen, in denen es um eine Vielzahl von Fragen geht: unlautere Geschäftspraktiken, Fernabsatz, Verbraucherkredit, Pauschalreisen, missbräuchliche Vertragsklauseln, Teilnutzungsrechte an Immobilien, elektronischer Geschäftsverkehr usw. Das CPCS kann nicht für den Informationsaustausch in Rechtsbereichen genutzt werden, die nicht ausdrücklich in diesem Anhang aufgeführt sind.

Beispiele:

I. Ein Händler in Belgien wendet gegenüber Verbrauchern aus Frankreich unfaire Praktiken an und verstößt damit gegen die Richtlinie über missbräuchliche Klauseln in Verbraucherverträgen. Nun kann die Verbraucherbehörde in Frankreich über das CPCS die Verbraucherbehörde in Belgien ersuchen, alle erforderlichen und in Belgien zulässigen Durchsetzungsmaßnahmen gegenüber dem Händler zu ergreifen, um den innergemeinschaftlichen Verstoß unverzüglich zu beenden.

II. Bei der Verbraucherbehörde in Dänemark gehen Beschwerden ein, wonach auf einer bestimmten Website betrügerische und irreführende Geschäftspraktiken zum Schaden der Verbraucher angewandt werden. Die Website wird von Schweden aus verwaltet. Die dänische Verbraucherbehörde benötigt Informationen über die Website. Über das CPCS kann sie ein Informationsersuchen an die schwedische Verbraucherbehörde richten, die die Auskünfte erteilen muss.

Die Informationen werden von den Mitgliedstaaten hochgeladen, im CPCS gespeichert, von den Mitgliedstaaten, an die die Informationen gerichtet sind, abgerufen und von der Kommission gelöscht [2]. Das CPCS wird als Informationsspeicher genutzt sowie als Instrument für den Informationsaustausch mittels eines effizienten und sicheren Kommunikationssystems.

Der Aufbau einer solchen Datenbank birgt immer gewisse Risiken für das grundlegende Recht auf den Schutz personenbezogener Daten: Es werden mehr Daten bereitgestellt, als für eine effiziente Zusammenarbeit unbedingt nötig sind, es bleiben Daten gespeichert, die hätten gelöscht werden sollen, und es werden Daten aufbewahrt, die nicht oder nicht mehr zutreffend sind, es gelingt nicht zu gewährleisten, dass die Rechte der betroffenen Personen gewahrt werden und dass die für die Verarbeitung Verantwortlichen ihre Pflichten erfüllen. Zur Abwendung dieser Risiken muss folglich sichergestellt werden, dass die CPCS-Nutzer in Datenschutzfragen gut informiert und geschult und dass sie in der Lage sind, die Einhaltung der geltenden Datenschutzvorschriften zu gewährleisten.

4. RECHTSRAHMEN UND KONTROLLE

Die Europäische Union verfügt seit 1995 über bewährte datenschutzrechtliche Rahmenvorschriften: Die Datenschutzrichtlinie [3] und die Datenschutzverordnung [4] regeln die Verarbeitung personenbezogener Daten durch die Mitgliedstaaten bzw. durch die Organe und Einrichtungen der Europäischen Union. Die Anwendung der Datenschutzvorschriften hängt zurzeit davon ab, wer der CPCS-Akteur oder -Nutzer ist.

---

[1] Die Datenschutzgrundsätze gelten für elektronisch gespeicherte Daten ebenso wie für Daten auf Papier.
[2] Genaue Bestimmungen für das Löschen von Daten enthalten die Entscheidung 2007/76/EG und das Dokument „Consumer Protection Cooperation Network: Operating Guidelines".
[3] Richtlinie 95/46/EG.
[4] Verordnung (EG) Nr. 45/2001.

Wenn die Kommission Daten verarbeitet, gilt die Datenschutzverordnung, wenn es die Sachbearbeiter in den zuständigen nationalen Durchsetzungsbehörden tun, gelten die nationalen Vorschriften bzw. Gesetze, mit denen die Datenschutzrichtlinie umgesetzt worden ist.

Als Hauptakteure mit spezifischen Aufgaben im CPCS sind sowohl die Kommission als auch die benannten zuständigen Behörden — als gemeinsame Kontrolleure — verpflichtet, ihre jeweiligen Datenverarbeitungsvorgänge den zuständigen Aufsichtsbehörden zur Vorabprüfung zu melden und zu übermitteln und die Einhaltung der Datenschutzbestimmungen zu gewährleisten. Die nationalen Vorschriften bzw. Gesetze, mit denen die Datenschutzrichtlinie umgesetzt worden ist, können Ausnahmen von den Bestimmungen im Zusammenhang mit Meldung und Vorabprüfung vorsehen.

Durch die Harmonisierung der Datenschutzbestimmungen sollen ein hohes Maß an Datenschutz gewährleistet, die Grundrechte des Einzelnen geschützt und zugleich ein ungehinderter Austausch personenbezogener Daten zwischen den Mitgliedstaaten ermöglicht werden. Da die nationalen Umsetzungsmaßnahmen zu Unterschieden bei den Bestimmungen geführt haben können und damit die Einhaltung der Datenschutzbestimmungen gewährleistet ist, wird den CPCS-Nutzern sehr empfohlen, diese Leitlinien mit der jeweiligen nationalen Datenschutzbehörde zu erörtern; es mag beispielsweise durchaus unterschiedliche Bestimmungen darüber geben, welche Informationen dem Einzelnen bereitgestellt oder welche Datenverarbeitungsvorgänge den Datenschutzbehörden gemeldet werden müssen.

Ein ganz wesentliches Merkmal des EU-Rechtsrahmens für den Datenschutz ist seine Kontrolle durch unabhängige Datenschutzbehörden. Die Bürger haben das Recht, sich mit Beschwerden an diese Behörden zu wenden, die ohne Einschaltung eines Gerichts umgehend auf die Datenschutzanliegen reagieren müssen. Die Verarbeitung personenbezogener Daten auf nationaler Ebene wird von den nationalen Datenschutzbehörden kontrolliert, die Verarbeitung personenbezogener Daten in den EU-Organen und -Einrichtungen vom Europäischen Datenschutzbeauftragten (EDSB) ([1]). Die Kommission untersteht somit der Aufsicht des EDSB, die anderen CPCS-Nutzer der ihrer nationalen Datenschutzbehörde.

5. WER MACHT WAS IM CPCS? DIE FRAGE DER GEMEINSAMEN KONTROLLE

Das CPCS ist ein gutes Beispiel für eine Anwendung mit gemeinsamen Datenverarbeitungsvorgängen und gemeinsamer Kontrolle. Während nur die zuständigen Behörden der Mitgliedstaaten personenbezogene Daten sammeln, erfassen, weitergeben und austauschen, ist die Kommission für das Speichern und Löschen der Daten auf bzw. von ihren Servern zuständig. Die Kommission hat keinen Zugriff auf diese personenbezogenen Daten, sondern gilt als der Systemmanager und -betreiber.

Die Aufgabenverteilung zwischen der Kommission und den Mitgliedstaaten stellt sich somit folgendermaßen dar:

— Jede zuständige Behörde ist für ihre eigenen Datenverarbeitungsaktivitäten verantwortlich.

— Die Kommission ist nicht Nutzer, sondern Betreiber des Systems und in erster Linie für die Wartung und die Sicherheit der Systemarchitektur verantwortlich. Sie hat jedoch auch Zugriff auf die Warnmeldungen, die Rückmeldungen und andere den Fall betreffende Informationen ([2]). Dieses Zugriffsrecht dient der Kommission dazu, die Anwendung der Verordnung über die Zusammenarbeit und die Anwendung der im Anhang der Verordnung aufgeführten Verbraucherschutzvorschriften zu kontrollieren und entsprechende Statistiken zu erstellen. Die Kommission hat jedoch keinen Zugriff auf die Informationen in den Amtshilfe- und Durchsetzungsersuchen, da diese nur an die mit dem betreffenden Fall befassten zuständigen Behörden der Mitgliedstaaten gerichtet sind. Gemäß der Verordnung über die Zusammenarbeit kann die Kommission einer zuständigen Behörde allerdings in bestimmten Streitsituationen helfen ([3]), und sie kann zur Beteiligung an einer koordinierten Untersuchung mit mindestens drei Mitgliedstaaten aufgefordert werden ([4]).

— Die CPCS-Akteure sind gemeinsam zuständig für die Zulässigkeit der Datenverarbeitung, für die Unterrichtungen und für das Recht auf Auskunft, Widerspruch und Berichtigung.

— Sowohl die Kommission als auch die zuständigen Behörden sind in ihrer Funktion als Kontrolleure einzeln dafür verantwortlich, dass die Bestimmungen für ihre Datenverarbeitungsvorgänge mit den Datenschutzbestimmungen vereinbar sind.

6. CPCS-AKTEURE UND CPCS-NUTZER

Innerhalb des CPCS gibt es verschiedene Zugangsprofile: Der Zugang zur Datenbank ist auf nur einen benannten Beamten der zuständigen Behörde (authentifizierten Nutzer) beschränkt, diesem zugewiesen und nicht übertragbar. Einem Antrag auf Zugang zum CPCS kann nur stattgegeben werden, wenn die zuständigen Behörden der Mitgliedstaaten die Namen der betreffenden Beamten bei der Kommission gemeldet haben. Das für den Zugang zum System erforderliche Login/Passwort ist bei der zentralen Verbindungsstelle erhältlich.

Nur Nutzer in den ersuchten und in den ersuchenden zuständigen Behörden haben uneingeschränkten Zugang zu sämtlichen Informationen, die im Zusammenhang mit einem bestimmten Fall ausgetauscht werden; hierzu gehören auch alle Anlagen in der CPCS-Akte. Die zentralen Verbindungsstellen haben nur einen Lesezugriff für die Schlüsselinformationen zu einem Fall, so dass sie die zuständige Behörde ermitteln können, an die ein Ersuchen weiterzuleiten ist. Vertrauliche Unterlagen, die einem Ersuchen oder einer Warnmeldung beigefügt sind, können sie nicht einsehen.

([1]) http://www.edps.europa.eu/EDPSWEB/edps/EDPS
([2]) Artikel 8, 9 und 15 der Verordnung (EG) Nr. 2006/2004.
([3]) Artikel 8 Absatz 5 der Verordnung (EG) Nr. 2006/2004.
([4]) Artikel 9 der Verordnung (EG) Nr. 2006/2004.

Bei Durchsetzungsfällen haben die Nutzer in allen zuständigen Behörden, die als zuständig für die Rechtsvorschriften gemeldet sind, gegen die verstoßen wurde, Zugriff auf allgemeine Informationen. Dies geschieht mit Hilfe der Meldungen. Diese Meldungen sollten eine grobe Beschreibung des Falls und keine personenbezogenen Daten enthalten. Für den Namen des Verkäufers oder Dienstleistungserbringers (sofern es sich dabei um eine natürliche Person handelt) kann es Ausnahmeregelungen geben.

Die Kommission hat keinen Zugriff auf Informations- und Durchsetzungsersuchen sowie auf vertrauliche Unterlagen, erhält aber die Meldungen und Warnmeldungen.

7. DATENSCHUTZGRUNDSÄTZE FÜR DEN INFORMATIONSAUSTAUSCH

Die CPCS-Nutzer in den Mitgliedstaaten dürfen personenbezogene Daten nur unter den Bedingungen und gemäß den Grundsätzen der Datenschutzrichtlinie verarbeiten. Der für die Verarbeitung Verantwortliche ist dafür verantwortlich, dass bei der Verarbeitung personenbezogener Daten im CPCS die Datenschutzgrundsätze eingehalten werden.

Es sei ferner darauf hingewiesen, dass auf das CPCS sowohl Bestimmungen für den vertraulichen Umgang mit Daten als auch Datenschutzbestimmungen anwendbar sind. Bestimmungen über die vertrauliche Behandlung und über die berufliche Schweigepflicht können auf Daten im Allgemeinen anwendbar sein, während Datenschutzbestimmungen auf personenbezogene Daten beschränkt sind.

Es gilt, sich bewusst zu machen, dass die CPCS-Nutzer in den Mitgliedstaaten auch für viele andere Datenverarbeitungsvorgänge zuständig und möglicherweise keine Datenschutzexperten sind. Die Einhaltung der Datenschutzbestimmungen im CPCS muss nicht unnötig kompliziert sein oder einen allzu hohen Verwaltungsaufwand bedeuten. Auch muss die Vorgehensweise nicht immer dieselbe sein. Die vorliegenden Leitlinien sind Empfehlungen für den Umgang mit personenbezogenen Daten, und es sei erneut darauf hingewiesen, dass nicht alle innerhalb des CPCS ausgetauschten Daten personenbezogener Natur sind.

Vor jedem Hochladen von Informationen in das CPCS müssen die Durchsetzungsbeamten prüfen, ob die zu übermittelnden personenbezogenen Daten für eine effiziente Zusammenarbeit tatsächlich notwendig sind und an wen sie die personenbezogenen Daten übermitteln. Die Durchsetzungsbeamten müssen sich die Frage stellen, ob die Empfänger diese Informationen für die Warnmeldung oder das Amtshilfeersuchen tatsächlich benötigen.

Die folgenden grundlegenden Datenschutzgrundsätze sollen den Durchsetzungsbeamten mit Zugang zum CPCS dabei helfen, jedes Mal, wenn sie personenbezogene Daten innerhalb des Systems verarbeiten, zu prüfen, ob die Datenschutzbestimmungen für die Verarbeitung personenbezogener Daten eingehalten werden. Die Durchsetzungsbeamten sollten außerdem beachten, dass es auf nationaler Ebene Ausnahmen und Beschränkungen betreffend die Anwendung der unten aufgeführten Datenschutzgrundsätze geben mag, und sich diesbezüglich an ihre nationalen Datenschutzbehörden wenden ([1]).

Welche Datenschutzgrundsätze sind zu befolgen?

Die allgemeinen Datenschutzgrundsätze, die vor jeder Verarbeitung personenbezogener Daten zu beachten sind, stammen aus der Datenschutzrichtlinie. Da diese Richtlinie in innerstaatliches Recht umgesetzt worden ist, werden die Sachbearbeiter erneut dazu aufgerufen, ihre nationalen Datenschutz-Aufsichtsbehörden bezüglich der Anwendung der unten aufgeführten Grundsätze zu konsultieren; außerdem wird ihnen empfohlen zu prüfen, ob es Ausnahmen oder Beschränkungen betreffend die Anwendung dieser Grundsätze gibt.

Grundsatz der Transparenz

Gemäß der Datenschutzrichtlinie hat die betroffene Person ein Recht darauf, unterrichtet zu werden, wenn ihre personenbezogenen Daten verarbeitet werden. Der für die Verarbeitung Verantwortliche muss ihren Namen und ihre Adresse, den Zweck der Datenverarbeitung, die Empfänger der Daten und alle sonstigen Informationen angeben, die gewährleisten, dass die Verarbeitung nach Treu und Glauben erfolgt ([2]).

Die Daten dürfen nur unter den folgenden Voraussetzungen verarbeitet werden ([3]):

— Die betroffene Person hat ihre Einwilligung gegeben;

— die Verarbeitung ist für die Erfüllung eines Vertrags oder für die Durchführung vorvertraglicher Maßnahmen erforderlich;

— die Verarbeitung ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich;

— die Verarbeitung ist für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich;

([1]) Artikel 11 Absatz 2 und Artikel 13 der Richtlinie 95/46/EG.
([2]) Artikel 10 und 11 der Richtlinie 95/46/EG.
([3]) Artikel 7 der Richtlinie 95/46/EG.

— die Verarbeitung ist erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem für die Verarbeitung Verantwortlichen oder einem Dritten, dem die Daten übermittelt werden, übertragen wurde;

— die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden.

Grundsatz der Rechtmäßigkeit und Grundsatz von Treu und Glauben

Personenbezogene Daten dürfen nicht auf unlautere oder unrechtmäßige Art und Weise erhoben oder verarbeitet noch für Zwecke verwendet werden, die mit denen in der Verordnung über die Zusammenarbeit nicht vereinbar sind. Damit die Verarbeitung rechtmäßig ist, müssen die Sachbearbeiter gute Gründe haben, die den Verarbeitungsbedarf rechtfertigen. Die Daten dürfen nur zu festgelegten, eindeutigen und rechtmäßigen Zwecken erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden ([1]). Diese Zwecke können sich nur aus der Verordnung über die Zusammenarbeit herleiten.

Damit die Verarbeitung „nach Treu und Glauben" geschieht, müssen die betroffenen Personen darüber unterrichtet werden, wozu ihre Daten verarbeitet werden sollen, sowie über ihre Auskunfts-, Berichtigungs- und Widerspruchsrechte.

Grundsatz der Verhältnismäßigkeit und Grundsatz der sachlichen Richtigkeit; Aufbewahrungsdauer

Die Informationen müssen den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein und dürfen nicht darüber hinausgehen. Die Daten müssen sachlich richtig und, wenn nötig, auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit im Hinblick auf die Zwecke, für die sie erhoben oder weiterverarbeitet werden, unrichtige oder unvollständige Daten gelöscht oder berichtigt werden; personenbezogene Daten müssen in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht, und dürfen nicht länger aufbewahrt werden, als es für die Zwecke, für die sie erhoben oder weiterverarbeitet wurden, erforderlich ist. Es sind geeignete Sicherheitsvorkehrungen für personenbezogene Daten vorzusehen, die über längere Zeit für historische, statistische oder wissenschaftliche Zwecke aufbewahrt werden.

Die Sachbearbeiter müssen prüfen, ob die Informationen, die sie verarbeiten, für den angestrebten Zweck tatsächlich nötig sind.

Eingrenzung des Zwecks

Personenbezogene Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; die betroffenen Personen sind hiervon zu unterrichten. Die Sachbearbeiter dürfen personenbezogene Daten nur verarbeiten, wenn der Zweck eindeutig ist, d. h., wenn die Verordnung über die Zusammenarbeit die rechtliche Grundlage für die Übermittlung liefert.

Zugangsrechte

Die betroffenen Personen haben gemäß der Datenschutzrichtlinie ([2]) das Recht, darüber unterrichtet zu werden, dass ihre personenbezogenen Daten verarbeitet werden, zu welchen Zwecken dies geschieht, wer die Empfänger der Daten sind und dass sie als betroffene Personen bestimmte Rechte haben, nämlich das Recht auf Unterrichtung und auf Berichtigung. Die betroffene Person hat das Recht auf Zugang zu allen sie betreffenden, verarbeiteten Daten. Die betroffene Person hat außerdem das Recht zu verlangen, dass Daten, die unvollständig oder unrichtig sind oder deren Verarbeitung nicht im Einklang mit den Datenschutzbestimmungen erfolgt ist, berichtigt, gelöscht oder gesperrt werden ([3]).

Sensible Daten

Untersagt ist die Verarbeitung von Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen und die Gewerkschaftszugehörigkeit hervorgehen, von Daten über Gesundheit und Sexualleben sowie von Daten, die Straftaten und strafrechtliche Verurteilungen betreffen. In der Datenschutzrichtlinie ([4]) ist allerdings vorgesehen, dass diese sensiblen Daten in gewissen Ausnahmefällen und unter bestimmten Voraussetzungen doch verarbeitet werden dürfen ([5]). CPCS-Nutzer, die mit sensiblen Daten ([6]) zu tun haben, sollten in jedem Fall vorsichtig damit umgehen. Den CPCS-Nutzern wird empfohlen, sich bei ihrer nationalen Datenschutzbehörde zu erkundigen, ob für die Bearbeitung sensibler Daten abweichende Bestimmungen gelten.

Ausnahmen

Im Zusammenhang mit der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten sieht die Datenschutzrichtlinie Ausnahmeregelungen vor. Den Sachbearbeitern wird empfohlen, ihre nationalen Vorschriften zu prüfen, um zu beurteilen, ob und in welchem Umfang solche Ausnahmeregelungen möglich sind ([7]). Falls solche Ausnahmeregelungen angewandt werden, wird empfohlen, sie klar und deutlich in der Datenschutzerklärung der jeweiligen zuständigen Behörde anzugeben.

([1]) Artikel 6 Absatz 1 Buchstabe b der Richtlinie 95/46/EG.
([2]) Artikel 10, 11 und 12 der Richtlinie 95/46/EG.
([3]) Artikel 12 der Richtlinie 95/46/EG.
([4]) Artikel 8 Absatz 2 der Richtlinie 95/46/EG.
([5]) Artikel 8 der Richtlinie 95/46/EG.
([6]) Kapitel 4 des Anhangs der Entscheidung 2007/76/EG.
([7]) Stellungnahme 6/2007 zu Datenschutzfragen im Zusammenhang mit dem Kooperationssystem für Verbraucherschutz (CPCS) 01910/2007/DE (WP 130), angenommen am 21. September 2007, S. 24-26.

Anwendung der Datenschutzgrundsätze

Bei der Anwendung dieser Datenschutzgrundsätze auf das CPCS ergeben sich folgende Empfehlungen:

1. Die Nutzung des CPCS sollte strikt auf die Zwecke beschränkt sein, die in der Verordnung über die Zusammenarbeit aufgeführt sind. In Artikel 13 Absatz 1 der Verordnung über die Zusammenarbeit heißt es, dass die übermittelten Informationen nur zu dem Zweck verwendet werden dürfen, die Einhaltung der Gesetze zum Schutz der Verbraucherinteressen zu gewährleisten. Diese „Gesetze" sind im Anhang der Verordnung über die Zusammenarbeit aufgelistet.

2. Den Durchsetzungsbeamten wird empfohlen, die Informationen, die sie im Rahmen eines Amtshilfeersuchens oder einer Warnmeldung erhalten, nur für die Zwecke des jeweiligen Falles zu verwenden, und zwar unter sorgfältiger Beachtung der Datenschutzvorschriften und nachdem sie zuvor geprüft haben, ob die Verarbeitung im Zusammenhang mit Ermittlungen, die in einem weiteren öffentlichen Interesse stattfinden, notwendig sind.

3. Anlässlich der Übermittlung von Daten prüfen die Durchsetzungsbeamten von Fall zu Fall, wer die zu verarbeitenden Informationen erhalten sollte.

4. Die CPCS-Nutzer sollten sich gut überlegen, welche Fragen sie im Rahmen eines Amtshilfeersuchens stellen, und nicht mehr Daten erfragen als nötig. Dies dient nicht nur der Datenqualität, sondern auch der Reduzierung des Verwaltungsaufwands.

5. Gemäß der Datenschutzrichtlinie ([1]) müssen personenbezogene Daten sachlich richtig und auf dem neuesten Stand sein. Die Empfehlung lautet, dass die zuständige Behörde, die die Informationen bereitgestellt hat, einen Beitrag dazu leisten sollte, dass die im CPCS gespeicherten Daten sachlich richtig sind. Mit Pop-up-Nachrichten im CPCS werden die Sachbearbeiter regelmäßig daran erinnert zu überprüfen, ob die personenbezogenen Daten noch sachlich richtig und aktuell sind.

6. Ein ausführlicher Datenschutzhinweis auf der Internetseite ist eine praktische Art und Weise, die betroffenen Personen über ihre Rechte zu informieren. Es wird empfohlen, dass jede zuständige Behörde einen solchen Hinweis auf ihren Internetseiten veröffentlicht. Alle Datenschutzhinweise sollten sämtlichen Informationspflichten der Datenschutzrichtlinie genügen, einen Link zur Internetseite der Kommission über Datenschutz enthalten sowie weitere Angaben, darunter die Kontaktdaten der betreffenden zuständigen Behörde und eventuelle nationale Beschränkungen des Rechts auf Auskunft oder auf Unterrichtung. Alle beteiligten für die Datenverarbeitung Verantwortlichen sind dafür zuständig, dass Datenschutzhinweise veröffentlicht werden.

7. Die betroffenen Personen können beantragen, Auskunft über ihre personenbezogenen Daten zu erhalten und dass Daten in mehr als einer Datenbank berichtigt oder gelöscht werden. Obwohl jede zuständige Behörde ebenso wie der für die Verarbeitung Verantwortliche selbst für ihre Datenverarbeitungsvorgänge zuständig ist, sollte bei Anträgen, die einen grenzüberschreitenden Fall betreffen, eine koordinierte Reaktion angestrebt werden. Für einen solchen Fall wird empfohlen, dass die zuständige Behörde die anderen betroffenen zuständigen Behörden vom Eingang des Antrags unterrichtet.

   Ist eine zuständige Behörde der Ansicht, dass das von anderen zuständigen Behörden durchgeführte Ermittlungs- oder Durchsetzungsverfahren dadurch beeinträchtigt würde, dass dem Antrag stattgegeben wird, so sollte erstere die letzteren um Stellungnahme bitten, bevor sie dem Antrag stattgibt.

   Die betroffenen Personen können ihren Antrag auch an die Kommission richten. Die Kommission kann einem Antrag nur insoweit stattgeben, als sie Zugriff auf die Daten hat. Nach dem Eingang eines Antrags sollte die Kommission die zuständige Behörde konsultieren, die die Informationen bereitgestellt hat. Wenn keine Einwände erhoben werden oder wenn die zuständige Behörde es versäumt, innerhalb eines angemessenen Zeitraums zu reagieren, kann die Kommission auf der Grundlage der Datenschutzverordnung entscheiden, dem Antrag stattzugeben oder ihn abzulehnen. Die Kommission sollte auch jene zuständigen Behörden um Stellungnahme bitten, deren Ermittlungs- oder Durchsetzungsaktivitäten beeinträchtigt werden könnten, falls dem Antrag stattgegeben wird. Die Kommission sollte prüfen, ob die Aufnahme zusätzlicher technischer Merkmale in das CPCS den Datenaustausch erleichtern würde.

8. In der Durchführungsentscheidung 2007/76/EG ist festgelegt, dass das CPCS Datenfelder für die Namen der Unternehmensleiter enthält. Die Durchsetzungsbeamten müssen prüfen, ob die Aufnahme solcher personenbezogener Daten zur Lösung des Falls erforderlich ist. Bevor Informationen in das CPCS hochgeladen werden und bevor eine Warnmeldung oder ein Amtshilfeersuchen an eine andere zuständige Behörde gerichtet wird, ist von Fall zu Fall zu prüfen, ob es nötig ist, den Namen des Unternehmensleiters in das dafür vorgesehene Datenfeld einzutragen.

9. Die Durchführungsentscheidung 2007/76/EG schreibt vor, dass die zuständige Behörde, die Informations- oder Durchsetzungsersuchen oder Warnmeldungen hochlädt, angeben muss, ob die Informationen vertraulich zu behandeln sind. Dies muss in jedem Einzelfall geschehen. Ebenso muss die ersuchte Behörde bei den bereitgestellten Informationen angeben, ob diese vertraulich zu behandeln sind. Aufgrund einer Standardeinstellung im CPCS müssen dessen Nutzer die Einstufung eines Dokuments als vertraulich ausdrücklich deaktivieren, um den Zugang zu einem Dokument zu gewähren.

([1]) Artikel 6 Artikel 1 Buchstabe d der Richtlinie 95/46/EG.

8. DAS CPCS UND DER DATENSCHUTZ

Eine datenschutzfreundliche Umgebung

Das CPCS ist unter Berücksichtigung von Datenschutzanforderungen konzipiert worden:

— Das CPCS nutzt s-TESTA (secured Trans European Services for Telematics between Administrations). Dies ist eine verwaltete, zuverlässige und sichere europaweite Kommunikationsplattform für europäische und nationale Verwaltungen. Das s-TESTA-Netz wird über eine eigene private Infrastruktur betrieben, die völlig getrennt vom Internet ist. Geeignete, in das System integrierte Sicherheitsvorkehrungen garantieren einen optimalen Schutz des Netzes. Das Netz unterliegt einer Sicherheitsakkreditierung, damit es für die Übermittlung von Informationen geeignet ist, die als „EU — Nur für den Dienstgebrauch" eingestuft sind.

— Es weist bestimmte technische Merkmale auf: sichere und personalisierte Passwörter für die gemeldeten zuständigen Beamten in den benannten Behörden; Nutzung eines sicheren Netzes (s-TESTA); Pop-up-Nachrichten, die die Sachbearbeiter dazu ermahnen, bei der Verarbeitung personenbezogener Daten die Datenschutzbestimmungen einzuhalten; Erstellung verschiedener Zugangsprofile für unterschiedliche Nutzer je nach ihrer Aufgabe (zuständige Behörde, zentrale Verbindungsstelle, Kommission); die Option, bestimmte Dokumente als vertraulich einzustufen und so die Zugriffsmöglichkeiten zu begrenzen; Verweis auf der CPCS-Homepage auf die Datenschutzbestimmungen.

— Durchführungsbestimmungen ([1]) zu Schlüsselaspekten zwecks Wahrung des Datenschutzes: klare Bestimmungen für das Löschen von Daten (was, wie, wann); Grundsätze für die Festlegung der Art des Zugriffs auf die Informationen (nur unmittelbar betroffene zuständige Behörden haben uneingeschränkten Zugang, die anderen erhalten nur allgemeine Informationen).

— Operationelle Leitlinien ([2]), aus denen deutlicher hervorgeht, was beim Ausfüllen der verschiedenen Datenfelder zu beachten ist, und Integration dieser Leitlinien ([3]).

— Jährliche Überprüfungen, um zu gewährleisten, dass die zuständigen Behörden die Richtigkeit der personenbezogenen Daten kontrollieren (eine Markierung (Tagging) ist geplant, aber noch nicht umgesetzt) und dass Fälle im Einklang mit den entsprechenden Bestimmungen geschlossen und/oder gelöscht werden, damit keine Fälle vergessen werden. Die Kommission veranstaltet mit den Mitgliedstaaten regelmäßig systematische Überprüfungen von Fällen, die überdurchschnittlich lange in Bearbeitung sind.

— Automatisches Löschen von Amtshilfefällen fünf Jahre nach Abschluss des Falls im Einklang mit der Verordnung über die Zusammenarbeit.

— Das CPCS ist eine in der Entwicklung befindliche IT-Anwendung, die datenschutzfreundlich sein möchte. Viele Sicherheitsmerkmale wurden bereits in die oben beschriebene Systemarchitektur aufgenommen. Die Kommission beabsichtigt auch künftig, bei Bedarf weitere Verbesserungen zu veranlassen.

Einige zusätzliche Hinweise

Wie lange sollte ein Fall gespeichert bleiben und wann sollte er abgeschlossen und gelöscht werden?

Nur die Kommission kann Informationen aus dem CPCS ([4]) löschen; dies geschieht in der Regel auf Antrag einer zuständigen Behörde. In einem solchen Antrag muss die zuständige Behörde die Gründe für ihr Ersuchen darlegen. Die einzige Ausnahme bilden Durchsetzungsersuchen. Diese werden von der Kommission automatisch fünf Jahre nach dem Zeitpunkt gelöscht, da die ersuchende Behörde den Fall abgeschlossen hat.

Es gibt Bestimmungen (mit Fristen), damit die Daten gelöscht werden, die nicht mehr erforderlich, unrichtig und/oder erwiesenermaßen nicht fundiert sind und/oder deren maximale Aufbewahrungsdauer erreicht ist.

Warum beträgt die Aufbewahrungsfrist fünf Jahre?

Die Aufbewahrungsfrist soll die Zusammenarbeit der bei innergemeinschaftlichen Verstößen gegen die Verbraucherschutzvorschriften zuständigen Durchsetzungsbehörden erleichtern sowie beitragen zum reibungslosen Funktionieren des Binnenmarkts, zur Qualität und Kohärenz der Durchsetzung der Verbraucherschutzvorschriften, zum Monitoring des Schutzes der wirtschaftlichen Interessen der Verbraucher sowie zur Steigerung von Qualität und Kohärenz der Durchsetzung. Während der Aufbewahrungsfrist dürfen befugte Durchsetzungsbeamte, die für eine zuständige Behörde arbeiten, welche ursprünglich mit dem Fall zu tun hatte, die Akte einsehen, um bei wiederholten Verstößen mögliche Zusammenhänge herzustellen; dies trägt zu einer besseren und effizienteren Durchsetzung bei.

([1]) Entscheidung 2007/76/EG.
([2]) The Consumer Protection Cooperation Network: Operating Guidelines; angenommen am 8. Juni 2010 durch den Ausschuss für die Zusammenarbeit im Verbraucherschutz.
([3]) Der Inhalt dieser Leitlinien wird in künftige CPCS-Schulungen einfließen.
([4]) Artikel 10 der Verordnung (EG) Nr. 2006/2004 und Kapitel 2 des Anhangs der Entscheidung 2007/76/EG.

Welche Informationen dürfen in das Diskussionsforum eingebracht werden?

Das Diskussionsforum ist ein Teil des CPCS und soll dem Austausch von Informationen über neue Durchsetzungsbefugnisse, bewährte Vorgehensweisen und ähnliche Themen dienen. Grundsätzlich sollte das Diskussionsforum, das nicht häufig von Durchsetzungsbeamten genutzt wird, nicht zum Austausch von Falldaten dienen und keine Verweise auf personenbezogene Daten enthalten.

Welche Art von Daten darf in die kurzen Zusammenfassungen und in die beigefügten Unterlagen aufgenommen werden?

In der Durchführungsentscheidung 2007/76/EG ist für Warnmeldungen sowie Informations- und Durchsetzungsersuchen das Datenfeld „Beigefügte Unterlagen" vorgesehen. Im Feld „Kurze Zusammenfassung" ist der Verstoß zu beschreiben. Es wird empfohlen, keine personenbezogenen Daten in die kurze Zusammenfassung aufzunehmen, da dieses Datenfeld eine allgemeine Beschreibung des Verstoßes bieten soll. Personenbezogene Daten in einer beigefügten Unterlage, die nicht unbedingt erforderlich sind, sollten geschwärzt oder entfernt werden.

Was ist gemeint mit „begründeter Verdacht, dass ein Verstoß begangen wurde"?

„Begründeter Verdacht" ist gemäß dem nationalen Recht auszulegen. Es wird jedoch empfohlen, mutmaßliche Verstöße nur dann in das CPCS aufzunehmen, wenn es Anhaltspunkte dafür gibt, dass ein Verstoß vorliegt oder wahrscheinlich vorliegt.

Was gilt für den Informationsaustausch mit Drittländern?

In der Verordnung über die Zusammenarbeit [1] heißt es, dass auf der Grundlage der Verordnung übermittelte Informationen im Rahmen eines Amtshilfeabkommens mit einem Drittland auch an eine Behörde dieses Drittlands übermittelt werden dürfen, sofern die Einwilligung der zuständigen Behörde, von der die Informationen ursprünglich stammen, eingeholt wurde und die Datenschutzvorschriften eingehalten werden.

Solange die Europäische Union noch keine internationale Übereinkunft über Einzelheiten der Amtshilfe geschlossen hat, wird empfohlen, dass bilaterale Amtshilfeabkommen [2] mit Drittländern angemessene Sicherheitsbestimmungen betreffend den Datenschutz enthalten und den zuständigen Datenschutz-Aufsichtsbehörden gemeldet werden, damit eine Vorabprüfung stattfinden kann; dies ist nicht nötig, wenn die Kommission befunden hat, dass das betreffende Drittland ein angemessenes Schutzniveau für aus der Union übermittelte personenbezogene Daten gemäß Artikel 25 der Datenschutzrichtlinie gewährleistet.

---

[1] Artikel 14 Absatz 2 der Verordnung (EG) Nr. 2006/2004.
[2] Artikel 18 der Verordnung (EG) Nr. 2006/2004.