RACCOMANDAZIONI

RACCOMANDAZIONE DELLA COMMISSIONE

del 1º marzo 2011

relativa alle linee guida per l'applicazione delle norme sulla protezione dei dati nell'ambito del Sistema di cooperazione per la tutela dei consumatori (CPCS)

(2011/136/UE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 292,

considerando quanto segue:

(1) Il regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio, del 27 ottobre 2004, sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa che tutela i consumatori («Regolamento sulla cooperazione per la tutela dei consumatori») [1] (in appresso «regolamento CPC») intende migliorare la cooperazione nell'applicazione delle norme che tutelano i consumatori all'interno del mercato unico, istituisce a livello dell'UE una rete di autorità pubbliche nazionali preposte all'esecuzione della normativa (in appresso «rete CPC») e stabilisce il quadro e le condizioni generali in cui tali autorità degli Stati membri cooperano per tutelare gli interessi economici collettivi dei consumatori.

(2) La cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa è essenziale per il funzionamento efficace del mercato unico e nell'ambito della rete CPC ciascuna autorità può chiedere l'assistenza delle altre autorità per accertare possibili violazioni della normativa UE sulla tutela dei consumatori.

(3) L'obiettivo del Sistema di cooperazione per la tutela dei consumatori (in appresso «CPCS») è consentire alle autorità pubbliche di esecuzione di scambiare informazioni riguardo a possibili violazioni delle norme sulla tutela dei consumatori in un ambiente sicuro.

(4) Lo scambio di informazioni mediante mezzi informatici tra gli Stati membri deve avvenire nel rispetto delle norme sulla protezione dei dati personali stabilite dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati [2] (in appresso «direttiva sulla protezione dei dati») e dal regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati [3] (in appresso «regolamento sulla protezione dei dati»).

(5) L'articolo 8 della Carta dei diritti fondamentali dell'Unione europea riconosce il diritto alla protezione dei dati. Il CPCS deve garantire che gli obblighi e le responsabilità della Commissione e degli Stati membri in materia di norme sulla protezione dei dati siano definiti chiaramente e che le persone interessate possano disporre di informazioni e di meccanismi facilmente accessibili per far valere i propri diritti.

(6) È opportuno stabilire linee guida per l'applicazione della normativa sulla protezione dei dati nell'ambito del CPCS (in appresso «linee guida»), al fine di garantire il rispetto delle norme sulla protezione dei dati durante il trattamento dei dati del CPCS.

(7) Gli agenti incaricati dell'applicazione della normativa dovrebbero essere invitati a contattare le autorità nazionali garanti della protezione dei dati per chiedere consulenza e assistenza sul modo migliore di applicare le linee guida in conformità alla legislazione nazionale e, se necessario, per assicurarsi che le procedure di notifica e di controllo preventivo relative alle operazioni di trattamento nell'ambito del CPCS siano messe in atto a livello nazionale.

(8) La partecipazione ai corsi di formazione organizzati dalla Commissione per facilitare l'applicazione delle linee guida va fortemente incoraggiata.

(9) Entro due anni dall'adozione della presente raccomandazione dovranno essere comunicate alla Commissione informazioni sull'applicazione delle linee guida. La Commissione dovrà poi procedere a un'ulteriore valutazione del livello di protezione dei dati nel CPCS e valutare se sono necessari strumenti supplementari, tra cui misure di regolamentazione.

[1] GU L 364 del 9.12.2004, pag. 1.
[2] GU L 281 del 23.11.1995, pag. 31.
[3] GU L 8 del 12.1.2001, pag. 1.

(10) Dovrebbero essere adottate le misure necessarie per facilitare l'attuazione delle linee guida da parte degli operatori e degli utilizzatori del CPCS. Le autorità nazionali garanti della protezione dei dati e il garante europeo della protezione dei dati dovrebbero monitorare attentamente l'evoluzione e l'attuazione dei meccanismi di protezione dei dati nell'ambito del CPCS.

(11) Le linee guida completano la decisione 2007/76/CE della Commissione [1] e tengono conto del parere del gruppo di lavoro per la tutela delle persone fisiche con riguardo al trattamento dei dati personali istituito dall'articolo 29 [2] della direttiva sulla protezione dei dati e del parere del garante europeo per la protezione dei dati [3] (in appresso «GEPD»), istituito dall'articolo 41 del regolamento sulla protezione dei dati,

HA ADOTTATO LA PRESENTE RACCOMANDAZIONE:

Gli Stati membri sono invitati a seguire le linee guida figuranti nell'allegato.

Fatto a Bruxelles, il 1º marzo 2011.

Per la Commissione
John DALLI
Membro della Commissione

[1] GU L 32 del 6.2.2007, pag. 192.
[2] Parere 6/2007 su temi riguardanti la protezione dei dati connessi con il Sistema di cooperazione per la tutela dei consumatori (CPCS) 01910/2007/EN — WP 130 — adottato il 21 settembre 2007.
[3] Parere del GEPD, rif. 2010-0692.

ALLEGATO

Linee guida per l'applicazione delle norme sulla protezione dei dati nell'ambito del Sistema di cooperazione per la tutela dei consumatori (CPCS)

1. INTRODUZIONE

La cooperazione tra le autorità nazionali responsabili della tutela dei consumatori è fondamentale per il buon funzionamento del mercato interno, perché un'applicazione inefficace della normativa nelle relazioni transfrontaliere mina la fiducia dei consumatori, che esitano ad accettare offerte transfrontaliere, e quindi mina la loro fede nel mercato interno e crea una distorsione della concorrenza.

Il CPCS è uno strumento informatico istituito dal regolamento CPC, che fornisce alle autorità nazionali responsabili della tutela dei consumatori facenti parte della rete CPC un meccanismo strutturato per lo scambio di informazioni. Esso permette a un'autorità pubblica di chiedere l'assistenza delle altre autorità pubbliche della rete CPC per individuare e trattare possibili violazioni della normativa UE sulla tutela dei consumatori e per adottare le misure destinate a mettere fine a pratiche commerciali illegali di venditori e fornitori nei confronti di consumatori che vivono in altri paesi dell'UE. Il CPCS è il mezzo utilizzato per le richieste di informazioni e per tutte le comunicazioni tra le autorità pubbliche competenti che riguardano l'applicazione del regolamento CPC.

Il regolamento CPC ha l'obiettivo di migliorare l'applicazione delle norme sulla tutela dei consumatori in tutto il mercato interno istituendo, a livello dell'UE, una rete delle autorità nazionali responsabili, nonché di definire le condizioni per la cooperazione fra gli Stati membri. Il regolamento CPC stabilisce che questi scambi di informazioni e le richieste di assistenza reciproca tra le autorità nazionali siano effettuati tramite una specifica banca dati. Il CPCS ha il compito di facilitare questa cooperazione amministrativa e lo scambio d'informazioni, ai fini dell'applicazione della normativa UE sulla protezione dei consumatori.

L'ambito della cooperazione è limitato alle infrazioni intracomunitarie degli atti giuridici elencati nell'allegato del regolamento CPC, che tutela gli interessi economici collettivi dei consumatori.

2. CAMPO DI APPLICAZIONE E OBIETTIVO DELLE LINEE GUIDA

Le presenti linee guida mirano soprattutto a garantire un equilibrio tra la cooperazione efficiente ed efficace delle autorità competenti dei vari Stati membri e il rispetto dei diritti fondamentali alla vita privata e alla protezione dei dati personali.

I dati personali sono definiti nella direttiva sulla protezione dei dati [1] come qualsiasi informazione concernente una persona fisica identificata o identificabile; si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero d'identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale.

Dato che gli agenti nazionali preposti all'applicazione della normativa («gli incaricati»), che sono gli utilizzatori del CPCS, non sono sempre esperti in materia di protezione dei dati e non hanno sempre una conoscenza sufficiente delle disposizioni della legislazione nazionale sulla protezione dei dati, è opportuno fornire agli utilizzatori del CPCS linee guida che illustrino il funzionamento del CPCS da un punto di vista pratico di protezione dei dati, nonché i meccanismi di salvaguardia del sistema e i possibili rischi legati al suo utilizzo.

L'obiettivo delle linee guida è trattare i temi più significativi della protezione dei dati nell'ambito del CPCS e fornire una spiegazione facilmente comprensibile a cui tutti gli utilizzatori del CPCS possano fare riferimento. Esse non forniscono, tuttavia, un'analisi dettagliata delle implicazioni del CPCS per la protezione dei dati.

Si raccomanda fortemente di consultare le autorità responsabili per la protezione dei dati degli Stati membri per completare le linee guida con gli obblighi specifici previsti dalla legislazione nazionale sulla protezione dei dati. Gli utilizzatori del CPCS possono inoltre ottenere dalle autorità nazionali garanti della protezione dei dati un'ulteriore assistenza e consulenza per accertare che siano rispettate le prescrizioni sulla protezione dei dati. Un elenco di queste autorità, con le loro coordinate e i siti web, può essere consultato su:

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

È chiaro che il trattamento dei dati personali va effettuato nel rispetto dei principi e delle condizioni specifiche stabiliti dalla direttiva sulla protezione dei dati. Nel contesto del regolamento, gli incaricati hanno il diritto di scambiare dati, anche di carattere personale, tramite il CPCS, se il trattamento ha lo scopo di mettere fine a una violazione delle norme UE sulla tutela dei consumatori, come indicato nell'allegato del regolamento CPC. Tuttavia, prima di trattare questi dati occorre esaminare attentamente se sono rispettati i principi della protezione dei dati e se il trattamento è assolutamente necessario per conseguire gli obiettivi del regolamento CPC.

[1] Articolo 2, lettera a).

Di conseguenza, gli incaricati che hanno accesso al CPCS dovranno esaminare ciascun caso singolarmente prima di poter procedere al trattamento dei dati personali [1]. Le presenti linee guida hanno lo scopo di assistere gli incaricati in questo esame fornendo alcuni principi direttivi da prendere in considerazione per la protezione dei dati.

Inoltre, le linee guida hanno l'obiettivo di chiarire alcune complessità della struttura del CPCS legate alle operazioni di trattamento e controllo congiunto, definendo il ruolo della Commissione e quello delle autorità competenti degli Stati membri come «controllori congiunti» degli scambi di dati tramite il CPCS.

3. IL CPCS — UNO STRUMENTO INFORMATICO PER LA COOPERAZIONE NELL'APPLICAZIONE DELLE NORME

Il CPCS è uno strumento informatico progettato e gestito dalla Commissione in cooperazione con gli Stati membri. Esso ha lo scopo di assistere gli Stati membri nell'applicazione pratica della normativa UE sulla tutela dei consumatori ed è utilizzato dalla rete CPC, costituita dalle autorità pubbliche designate dagli Stati membri e dai paesi del SEE, per collaborare e scambiare informazioni sull'applicazione delle norme relative alla tutela dei consumatori, come stabilito dal regolamento CPC.

L'articolo 10 del regolamento CPC recita:

«La Commissione mantiene una banca dati informatica in cui memorizza ed elabora le informazioni pervenute ai sensi degli articoli 7, 8 e 9. La banca dati può essere consultata soltanto dalle autorità competenti…»

L'articolo 12, paragrafo 3, del regolamento CPC stabilisce inoltre:

«Le richieste di assistenza e tutte le trasmissioni delle informazioni sono effettuate per iscritto, mediante un modello standard, e sono comunicate per via elettronica tramite la banca dati di cui all'articolo 10.»

Il CPCS facilita la cooperazione e gli scambi d'informazioni limitati alle infrazioni intracomunitarie delle direttive e dei regolamenti elencati nell'allegato del regolamento CPC che riguarda varie questioni, tra cui le pratiche commerciali sleali, le vendite a distanza, i crediti al consumo, i viaggi «tutto compreso», le clausole contrattuali abusive, le multiproprietà, il commercio informatico, ecc. Il CPCS non può essere utilizzato per scambi di informazioni in ambiti legislativi non specificati nell'allegato.

Esempi:

I. Un commerciante stabilito in Belgio utilizza clausole abusive nelle sue operazioni con i consumatori residenti in Francia, in violazione della direttiva sulle clausole contrattuali abusive. L'autorità francese responsabile dei consumatori può utilizzare il CPCS per chiedere all'autorità belga responsabile dei consumatori di adottare tutte le misure di applicazione necessarie, disponibili in Belgio, nei confronti del commerciante per mettere fine al più presto all'infrazione intracomunitaria.

II. L'autorità danese responsabile dei consumatori riceve denuncie secondo cui un particolare sito web ricorre a pratiche commerciali fraudolente e ingannevoli ai danni dei consumatori. Il sito web è ospitato in Svezia. L'autorità danese dei consumatori ha bisogno di informazioni sul sito web e può quindi utilizzare il CPCS per presentare una richiesta d'informazioni all'autorità svedese responsabile dei consumatori, che ha l'obbligo di fornire le informazioni.

Le informazioni sono trasmesse elettronicamente dagli Stati membri, memorizzate nel CPCS, consultate dagli Stati membri a cui l'informazione era destinata e cancellate dalla Commissione [2]. Il CPCS è utilizzato come repertorio di informazioni e come mezzo di scambio di informazioni tramite un sistema di comunicazione efficiente e sicuro.

Dal punto di vista della protezione dei dati, l'istituzione di una banca dati di questo tipo comporta sempre certi rischi per il diritto fondamentale alla protezione dei dati personali: la condivisione di un numero maggiore di dati di quello strettamente necessario per un'efficiente collaborazione; la conservazione di dati che avrebbero dovuto essere cancellati e che non sono più esatti o corretti; il mancato rispetto dei diritti delle persone interessate e degli obblighi dei responsabili del trattamento. È necessario perciò affrontare questi rischi assicurandosi che gli utilizzatori del CPCS abbiano una buona conoscenza delle norme di protezione dei dati e che siano in grado di garantire il rispetto della legislazione applicabile in materia di protezione dei dati.

4. PROTEZIONE DEI DATI: QUADRO GIURIDICO E DI CONTROLLO

L'Unione europea dispone di un quadro giuridico sulla protezione dei dati dal 1995: la direttiva sulla protezione dei dati [3], che disciplina il trattamento dei dati personali da parte degli Stati membri, e il regolamento sulla protezione dei dati [4], che disciplina il trattamento dei dati personali da parte delle istituzioni e dagli organismi dell'Unione europea. L'applicazione della normativa sulla protezione dei dati dipende attualmente dall'identità degli operatori e degli utilizzatori del CPCS.

---

[1] Va notato che i principi di protezione dei dati si applicano sia ai dati archiviati elettronicamente sia ai dati archiviati su supporto cartaceo.

[2] Per le norme specifiche relative alla cancellazione cfr. decisione 2007/76/CE e «Rete di cooperazione per la tutela dei consumatori: Linee guida generali».

[3] Direttiva 95/46/CE.

[4] Regolamento (CE) n. 45/2001.

Le operazioni di trattamento dei dati effettuate dalla Commissione sono disciplinate dal regolamento sulla protezione dei dati e quelle effettuate dagli operatori delle autorità nazionali sono disciplinate dalle leggi nazionali che recepiscono la direttiva sulla protezione dei dati.

Poiché la Commissione e le autorità competenti designate sono, come controllori congiunti, i due principali operatori con ruoli specifici nel CPCS, hanno l'obbligo di notificare alle autorità di controllo pertinenti e di sottoporre al loro controllo preliminare le rispettive operazioni di trattamento e di agire in conformità alle norme sulla protezione dei dati. Le leggi nazionali che recepiscono la direttiva sulla protezione dei dati possono tuttavia prevedere deroghe all'obbligo di notifica e di controllo preliminare.

L'armonizzazione delle leggi sulla protezione dei dati era intesa a garantire un livello elevato di protezione dei dati e la tutela dei diritti fondamentali delle persone, e contemporaneamente a consentire la libera circolazione dei dati personali tra gli Stati membri. Dato che le misure nazionali di attuazione possono comportare norme divergenti, si raccomanda fortemente agli utilizzatori del CPCS, al fine di garantire la conformità alla normativa sulla protezione dei dati, di discutere delle presenti linee guida con le autorità nazionali garanti della protezione dei dati, poiché le norme possono variare, ad esempio, per quanto riguarda le informazioni da fornire alle persone fisiche o l'obbligo di notifica di determinate operazioni di trattamento dei dati alle autorità di protezione dei dati.

Una caratteristica importante del quadro giuridico dell'UE in materia di protezione dei dati è il controllo di autorità indipendenti responsabili della protezione dei dati. I cittadini hanno il diritto di presentare denunce a tali autorità e di ottenere che i loro problemi in materia di protezione dei dati siano risolti prontamente in un contesto extragiudiziale. A livello nazionale, il trattamento dei dati personali è controllato dalle autorità nazionali garanti della protezione dei dati, mentre a livello delle istituzioni europee il trattamento dei dati personali è controllato dal garante europeo della protezione dei dati (GEPD) ([1]). Di conseguenza, la Commissione è soggetta al controllo del GEPD mentre gli altri utilizzatori del CPCS sono soggetti al controllo delle autorità nazionali di controllo competenti in materia di protezione dei dati.

5. CHI FA COSA NEL CPCS? — LA QUESTIONE DEL CONTROLLO CONGIUNTO

Il CPCS costituisce un chiaro esempio di operazioni di trattamento e di controllo congiunte. Mentre solo le autorità competenti degli Stati membri possono raccogliere, registrare, comunicare e scambiare dati personali, la conservazione e la cancellazione di questi dati sui suoi server competono alla Commissione. Essa non ha accesso ai dati personali, ma è considerata l'amministratore e l'operatore del sistema.

Di conseguenza, la ripartizione dei diversi compiti e delle responsabilità tra la Commissione e gli Stati membri può essere riassunta come segue:

— ciascuna autorità competente svolge il ruolo di responsabile del trattamento per quanto riguarda le proprie attività di trattamento dei dati,

— la Commissione non è un utilizzatore, bensì l'operatore del sistema, responsabile in primo luogo della manutenzione e della sicurezza della struttura del sistema. Tuttavia, la Commissione ha anche accesso ad allarmi, informazioni di seguito e altri dati relativi ai casi trattati ([2]). L'accesso della Commissione ha come scopo il controllo dell'applicazione del regolamento CPC e della normativa, indicata nel suo allegato, concernente la tutela dei consumatori nonché la compilazione dei dati statistici relativi all'esecuzione di questi compiti. La Commissione non ha però accesso alle informazioni contenute nelle richieste di assistenza reciproca e di intervento, poiché queste sono destinate unicamente alle autorità competenti degli Stati membri che trattano lo specifico caso in questione. Il regolamento CPC prevede tuttavia la possibilità che la Commissione assista le autorità competenti in caso di controversia ([3]) e che sia invitata a partecipare a inchieste coordinate svolte da più di due Stati membri ([4]),

— gli operatori del CPCS condividono la responsabilità per quanto riguarda la legittimità del trattamento dei dati, la fornitura di informazioni e i diritti di accesso, obiezione e rettifica,

— la Commissione e le autorità competenti, nel loro ruolo di responsabili del trattamento, hanno ciascuna la responsabilità di assicurare il controllo che le norme applicate alle loro operazioni di trattamento dei dati siano compatibili con le norme sulla protezione dei dati.

6. OPERATORI E UTILIZZATORI DEL CPCS

Il CPCS prevede diversi tipi di accesso: l'accesso alla banca dati è limitato, è riservato a un agente designato dell'autorità competente (utilizzatore autenticato) e non è trasferibile. L'accesso al CPCS può essere concesso solo agli agenti notificati alla Commissione dalle autorità competenti degli Stati membri. Per entrare nel sistema è necessario un login/password, che può essere ottenuto presso l'ufficio di collegamento unico.

Solo gli utilizzatori delle autorità competenti richiedenti o interpellate hanno pieno accesso all'insieme di informazioni scambiate per un dato caso, comprendente tutti i documenti relativi alla pratica contenuti nel CPCS. Gli uffici di collegamento unici possono solo leggere le informazioni principali su un dato caso, in modo da poter identificare l'autorità competente cui deve essere inviata una richiesta. Essi non possono leggere i documenti riservati allegati a una richiesta o a un allarme.

([1]) http://www.edps.europa.eu/EDPSWEB/edps/EDPS
([2]) Articoli 8, 9, e 15 del regolamento CPC (CE) n. 2006/2004.
([3]) Articolo 8, paragrafo 5, del regolamento CPC (CE) n. 2006/2004.
([4]) Articolo 9 del regolamento CPC (CE) n. 2006/2004.

Nei casi di intervento, le informazioni generali sono condivise tra gli utilizzatori di tutte le autorità competenti indicate come responsabili per il caso di violazione in questione. Ciò avviene tramite notifiche, che descrivono brevemente il caso evitando di indicare dati personali. Possono essere fatte eccezioni per quanto riguarda il nome del venditore o del fornitore (se si tratta di una persona fisica).

La Commissione non ha accesso alle richieste di informazione e di intervento o ai documenti riservati, ma riceve comunque notifiche e allarmi.

7. PRINCIPI DI PROTEZIONE DEI DATI APPLICABILI AGLI SCAMBI DI INFORMAZIONI

Il trattamento di dati personali da parte degli utilizzatori del CPCS negli Stati membri può essere effettuato solo a determinate condizioni e in conformità ai principi stabiliti dalla direttiva sulla protezione dei dati. Il responsabile del trattamento ha il compito di garantire il rispetto dei principi di protezione dei dati durante il trattamento dei dati personali nel CPCS.

Va inoltre notato che il CPCS è soggetto sia alle norme sulla riservatezza sia a quelle sulla protezione dei dati. Le norme relative alla riservatezza e al segreto professionale possono essere applicate ai dati in generale, mentre le norme sulla protezione dei dati sono limitate ai dati personali.

È importante tenere presente che, negli Stati membri, gli utilizzatori del CPCS sono responsabili di molte altre operazioni di trattamento e possono non essere esperti in materia di protezione dei dati. Il rispetto della protezione dei dati nel CPCS non deve essere inutilmente complicato o comportare un onere amministrativo eccessivo. Non deve nemmeno consistere in un sistema unico universalmente valido. Le presenti linee guida sono raccomandazioni per il trattamento dei dati personali e va ricordato che non tutti i dati scambiati con il CPCS sono necessariamente dati personali.

Prima di trasmettere le informazioni al CPCS, gli agenti preposti all'applicazione della normativa devono esaminare se i dati personali da inviare sono assolutamente necessari per un'efficiente cooperazione e considerare chi è il destinatario a cui inviano i dati personali. L'agente deve chiedersi se il destinatario riceve queste informazioni unicamente ai fini dell'allarme o della richiesta di assistenza reciproca.

Si richiamano qui di seguito i principi fondamentali di protezione dei dati; in base ad essi, gli agenti che hanno accesso al CPCS potranno valutare caso per caso se le norme sulla protezione dei dati relative al trattamento dei dati personali sono rispettate ogni volta che trattano dati personali nel sistema. Gli agenti devono anche tenere conto del fatto che l'applicazione dei principi di protezione dei dati può essere soggetta a deroghe e limitazioni a livello nazionale e quindi si consiglia loro di consultare le autorità nazionali garanti della protezione dei dati [1].

Quali sono i principi di protezione dei dati da osservare?

I principi generali di protezione dei dati da prendere in considerazione prima del trattamento di qualsiasi dato personale sono quelli stabiliti dalla direttiva sulla protezione dei dati. Dato che questa direttiva è stata recepita nella legislazione nazionale, si ricorda agli incaricati di consultare le autorità nazionali garanti della protezione dei dati riguardo all'applicazione dei principi sottoelencati e di verificare se esistono deroghe e limitazioni alla loro applicazione.

Trasparenza

Secondo la direttiva sulla protezione dei dati, la persona i cui dati personali sono oggetto di un trattamento ha il diritto di esserne informata. Il responsabile del trattamento è tenuto a indicare il proprio nome e indirizzo, le finalità del trattamento, i destinatari dei dati e tutte le altre informazioni richieste per garantire un trattamento dei dati leale [2].

I dati possono essere trattati solo nelle seguenti circostanze [3]:

— se la persona interessata ha dato il proprio consenso,

— se il trattamento è necessario all'esecuzione o alla conclusione di un contratto,

— se il trattamento è necessario per adempiere un obbligo legale,

— se il trattamento è necessario per la salvaguardia di interessi vitali delle persona interessata,

[1] Articolo 11, paragrafo 2, e articolo 13 della direttiva 95/46/CE.
[2] Articoli 10 e 11 della direttiva 95/46/CE.
[3] Articolo 7 della direttiva 95/46/CE.

— se il trattamento è necessario per l'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il responsabile del trattamento o il terzo cui vengono comunicati i dati,

— se il trattamento è necessario per perseguire gli interessi legittimi del responsabile del trattamento o dei terzi cui vengono comunicati i dati.

Trattamento lecito e leale

I dati personali non possono essere raccolti o trattati in modo sleale o illecito e non devono essere utilizzati per fini incompatibili con quelli stabiliti dal regolamento CPC. Affinché il trattamento sia lecito, i responsabili del trattamento devono assicurarsi che esistano motivi che giustificano chiaramente la necessità del trattamento. Esso deve essere effettuato per finalità determinate, esplicite e legittime e i dati non possono essere successivamente trattati in modo incompatibile con tali finalità ([1]). Questi motivi possono essere stabiliti solo nel regolamento CPC.

Affinché il trattamento sia leale, le persone interessate devono essere informate delle finalità per le quali i loro dati vengono trattati e dell'esistenza del diritto di accesso, rettifica e obiezione.

Proporzionalità, esattezza e periodo di conservazione

Le informazioni devono essere proporzionate, adeguate, pertinenti e non eccessive rispetto alle finalità per le quali vengono raccolte e/o trattate successivamente. I dati devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per garantire che i dati inesatti o incompleti siano cancellati o rettificati, considerando le finalità per le quali sono stati raccolti o trattati successivamente; i dati personali vanno conservati in una forma che consenta l'identificazione delle persone interessate, per un periodo non superiore al tempo necessario per realizzare le finalità per le quali i dati sono stati raccolti o trattati. Garanzie adeguate devono essere previste per i dati personali conservati per periodi più lunghi per motivi storici, statistici o scientifici.

I responsabili del trattamento devono verificare se le informazioni che trattano sono strettamente necessarie per le finalità perseguite.

Limitazione della finalità

I dati personali devono essere raccolti per finalità determinate, esplicite e legittime e non possono essere trattati successivamente in modo incompatibile con tali finalità, inizialmente specificate alla persona interessata. I responsabili del trattamento possono trattare i dati personali solo se esiste una chiara finalità per farlo, vale a dire se il regolamento CPC prevede ragioni giuridiche che giustificano il trasferimento dei dati.

Diritti di accesso

In base alla direttiva sulla protezione dei dati ([2]), le persone interessate hanno il diritto di essere informate del trattamento dei loro dati personali, delle finalità del trattamento, dei destinatari dei dati e del fatto che hanno specifici diritti, come il diritto di informazione e di rettifica. La persona interessata ha il diritto di accesso a tutti i dati trattati che la riguardano. Essa ha anche il diritto di chiedere la rettifica, la cancellazione o il congelamento dei dati che sono incompleti, inesatti o che non sono trattati conformemente alle norme sulla protezione dei dati ([3]).

Dati sensibili

È vietato il trattamento di dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale nonché dei dati relativi alla salute e alla vita sessuale, alle infrazioni e alle condanne penali. La direttiva sulla protezione dei dati ([4]) prevede tuttavia alcune eccezioni a questa regola, che consentono il trattamento dei dati sensibili in determinate condizioni ([5]). Dato che gli utilizzatori del CPCS possono trovarsi in una situazione in cui devono trattare dati sensibili ([6]), si consiglia loro di trattarli con prudenza. Si raccomanda di consultare l'autorità nazionale garante della protezione dei dati per sapere se sono previste deroghe per il trattamento dei dati sensibili.

Esenzioni

Nel contesto della prevenzione, dell'indagine, dell'individuazione e del perseguimento dei reati penali, la direttiva sulla protezione dei dati prevede alcune esenzioni. Si consiglia agli incaricati di consultare la legislazione nazionale per verificare se tali esenzioni sono possibili e in quale misura ([7]). In caso di ricorso alle esenzioni, si raccomanda di indicarle chiaramente nelle dichiarazioni sulla riservatezza di ciascuna autorità competente.

([1]) Articolo 6, paragrafo 1, lettera b), della direttiva 95/46/CE.
([2]) Articoli 10, 11 e 12 della direttiva 95/46/CE.
([3]) Articolo 12 della direttiva 95/46/CE.
([4]) Articolo 8, paragrafo 2, della direttiva 95/46/CE.
([5]) Articolo 8 della direttiva 95/46/CE.
([6]) Capitolo 4 dell'allegato della decisione 2007/76/CE.
([7]) Parere 6/2007 su temi riguardanti la protezione dei dati connessi con il Sistema di cooperazione per la tutela dei consumatori (CPCS) 01910/2007/EN — WP 130 — adottato il 21 settembre 2007, pagg. 24-26.

Applicazione dei principi di protezione dei dati

Per quanto riguarda l'applicazione dei principi di protezione dei dati al funzionamento del CPCS, si raccomanda quanto segue.

(1) L'utilizzo del CPCS deve essere strettamente limitato alle finalità previste nel regolamento CPC. L'articolo 13, paragrafo 1, del regolamento CPC stabilisce che le informazioni comunicate possono essere utilizzate esclusivamente allo scopo di garantire il rispetto della normativa sulla protezione degli interessi dei consumatori. Gli atti relativi sono elencati nell'allegato del regolamento CPC.

(2) Si raccomanda agli agenti di utilizzare le informazioni ottenute grazie a una richiesta di assistenza reciproca o a un allarme solo per le finalità legate a quello specifico caso, osservando le disposizioni giuridiche relative alla protezione dei dati, dopo aver valutato la necessità del trattamento dei dati nel contesto delle indagini svolte nell'interesse pubblico generale.

(3) Quando trasferiscono i dati, gli agenti valutano caso per caso chi saranno i destinatari delle informazioni da trattare.

(4) Gli utilizzatori del CPCS devono scegliere attentamente le domande da porre nella richiesta di assistenza reciproca e non possono chiedere un numero di dati maggiore del necessario. Non si tratta solo di una questione di rispetto dei principi di qualità dei dati, ma anche di problema di riduzione dell'onere amministrativo.

(5) La direttiva sulla protezione dei dati [1] stabilisce che i dati personali devono essere esatti e aggiornati. L'autorità competente che ha fornito le informazioni dovrebbe contribuire a garantire l'esattezza dei dati conservati nel CPCS. Per ricordare periodicamente agli agenti di controllare se i dati personali sono esatti e aggiornati sono stati aggiunti messaggi pop-up nel CPCS.

(6) Un modo pratico per informare dei loro diritti le persone interessate consiste nel creare una pagina web con un'avvertenza dettagliata sulla riservatezza. Si raccomanda che ciascuna autorità competente provveda a dotare il suo sito web di un'avvertenza sulla riservatezza. Ogni avvertenza sulla riservatezza deve essere conforme a tutti gli obblighi d'informazione stabiliti dalla direttiva sulla protezione dei dati, essere provvista di un link verso la pagina web della Commissione sulla riservatezza e fornire dettagli complementari, come le coordinate dell'autorità competente interessata e le limitazioni nazionali del diritto di accesso o di informazione. Spetta a tutti i responsabili del trattamento provvedere affinché le avvertenze sulla riservatezza siano pubblicate.

(7) Le persone interessate possono chiedere l'accesso, la rettifica e la cancellazione dei loro dati personali da più di una fonte. Anche se ciascuna autorità competente, assume, in quanto responsabile del trattamento, la responsabilità delle proprie operazioni di trattamento dei dati, è opportuno che venga prevista una risposta coordinata alle richieste relative ai casi transfrontalieri. In questi casi, si raccomanda alle autorità competenti di comunicare alle autorità competenti interessate il ricevimento della richiesta.

Se un'autorità competente ritiene che l'accettazione di una richiesta possa influire sulla procedura di indagine o di intervento messa in atto da altre autorità competenti, dovrebbe chiedere il parere di queste altre autorità prima di accettare la richiesta.

La persona interessata può anche rivolgere una richiesta alla Commissione, la quale può accettare solo una richiesta riguardante dati a cui ha accesso. Quando riceve una richiesta, la Commissione deve consultare l'autorità competente che ha fornito l'informazione. Se non vengono sollevate obiezioni o se l'autorità competente non risponde entro un termine ragionevole, la Commissione può decidere di accettare la richiesta o di rifiutarla in base al regolamento sulla protezione dei dati. La Commissione dovrebbe anche chiedere il parere delle autorità competenti le cui attività di indagine o di esecuzione possono risultare compromesse dall'accettazione della richiesta. Inoltre, essa dovrebbe esaminare se l'inserimento di funzionalità tecniche aggiuntive nel CPCS potrebbe facilitare questi scambi.

(8) La decisione 2007/76/CE recante attuazione del regolamento CPC prevede campi di informazione nel CPCS per i nomi dei direttori delle imprese. Gli agenti devono valutare se l'inclusione di questo tipo di dati personali è necessario per risolvere la questione. Occorre valutare caso per caso se è necessario includere il nome del direttore di un'impresa nel campo di informazione previsto a tal fine, prima di trasmettere le informazioni al CPCS e prima di inviare un allarme o una richiesta di assistenza reciproca a un'altra autorità competente.

(9) La decisione 2007/76/CE recante attuazione del regolamento CPC stabilisce che l'autorità competente che trasmette informazioni o richieste di esecuzione o allarmi deve indicare se le informazioni vanno trattate in modo riservato. Questa decisione va presa caso per caso. Parallelamente, l'autorità interpellata deve indicare, quando fornisce l'informazione, se questa va trattata in modo riservato. Il CPCS è provvisto di una funzionalità per difetto che indica il carattere riservato dei documenti; gli utilizzatori devono autorizzare esplicitamente l'accesso, disattivando la funzionalità.

[1] Articolo 6, paragrafo1, lettera d), della direttiva 95/46/CE.

8. CPCS E PROTEZIONE DEI DATI

Un ambiente di facile uso per la protezione dei dati

Il CPCS è stato concepito tenendo presente la legislazione in materia di protezione dei dati:

— Il CPCS utilizza la rete di servizi transeuropei sicuri per la comunicazione telematica tra amministrazioni «s-TESTA» (secured Trans European Services for Telematics between Administrations). Questa rete costituisce una piattaforma di comunicazione paneuropea controllata, affidabile e sicura per le amministrazioni europee e nazionali. La rete s-TESTA si basa su un'infrastruttura privata specifica, completamente separata da Internet. Nella concezione del sistema sono incluse misure di sicurezza appropriate che garantiscono la migliore protezione possibile della rete. Essa è soggetta a un accreditamento in materia di sicurezza che la rende adatta alla trasmissione di informazioni classificate «EU Restricted».

— Nel sistema è stata introdotta una serie di caratteristiche tecniche: password sicure e personalizzate sono state notificate ai responsabili delle autorità designate, la rete utilizzata è protetta (s-TESTA), messaggi pop-up ricordano agli incaricati che devono tener conto delle norme di protezione dei dati quando effettuano il trattamento dei dati personali, sono stati creati diversi profili di utilizzatori per regolare l'accesso alle informazioni secondo il ruolo dell'utilizzatore (l'autorità competente, l'ufficio di collegamento unico o la Commissione), è stata prevista la possibilità di limitare l'accesso ai documenti definendoli riservati e sulla homepage del CPCS figura un messaggio che rimanda alle norme di protezione dei dati.

— Le regole di attuazione ([1]) coprono gli aspetti principali per garantire il rispetto della protezione dei dati: regole di cancellazione chiare (quali informazioni, come e quando cancellare dati); principi che specificano i tipi di accesso all'informazione (solo le autorità competenti direttamente interessate hanno pieno accesso mentre le altre autorità dispongono solo di informazioni generali).

— Linee guida operative ([2]) offrono chiarimenti complementari su cosa occorre prendere in considerazione nella compilazione dei vari campi di informazione, e in particolare le presenti linee guida ([3]).

— Revisioni annuali sono previste per dar modo alle autorità competenti di verificare l'esattezza dei dati personali (una classificazione è prevista, ma non è ancora stata applicata) e chiudere e/o cancellare i casi trattati, come previsto dalle norme per evitare che i casi siano «dimenticati». La Commissione organizza periodicamente con gli Stati membri una revisione sistematica dei casi aperti da un periodo notevolmente superiore alla media.

— È stato messo in atto un sistema automatico di cancellazione dei casi di assistenza reciproca 5 anni dopo la chiusura del caso, come richiesto dal regolamento CPC.

— Il CPCS è una strumento informatico in evoluzione che ha lo scopo di facilitare la protezione dei dati. Molte funzioni di protezione sono già state inserite nella struttura del sistema, come descritto sopra. La Commissione intende continuare a migliorare il sistema, secondo le esigenze che si presentano.

Altre indicazioni

Per quanto tempo un caso deve essere conservato e quando deve essere chiuso e cancellato?

Solo la Commissione può cancellare le informazioni del CPCS ([4]) e normalmente lo fa su richiesta di un'autorità competente. Quando presenta tale richiesta, l'autorità competente deve precisarne i motivi. Le richieste di intervento sono l'unica eccezione: sono cancellate automaticamente dalla Commissione 5 anni dopo la chiusura del caso da parte dell'autorità richiedente.

Esistono regole che prevedono termini specifici per garantire la cancellazione di dati non più richiesti, inesatti, infondati e/o conservati per un periodo massimo.

Perché il periodo di conservazione dei dati è stato fissato in 5 anni?

Lo scopo del periodo di conservazione è facilitare la cooperazione fra le autorità pubbliche, responsabili dell'esecuzione della normativa in materia di tutela degli interessi dei consumatori, nel trattamento delle infrazioni intracomunitarie, contribuire al buon funzionamento del mercato interno, al miglioramento della qualità e della coerenza dell'applicazione delle leggi che tutelano gli interessi dei consumatori, al monitoraggio della protezione degli interessi economici dei consumatori e contribuire ad accrescere l'efficacia e la coerenza degli interventi. Durante il periodo di conservazione, gli agenti che lavorano per un'autorità competente a cui un dato caso è stato inizialmente affidato possono consultare la pratica in questione per verificare i legami con eventuali infrazioni ripetute, in modo da migliorare e rendere più efficiente l'azione di contrasto.

([1]) Decisione 2007/76/CE
([2]) *The Consumer Protection Cooperation Network: Operating Guidelines* (Rete per la cooperazione nella tutela dei consumatori: linee guida operative) — approvato dal comitato CPC l'8 giugno 2010.
([3]) Il contenuto di queste linee guida sarà inserito nelle formazioni future sul CPCS.
([4]) Articolo 10 del regolamento CPC (CE) n. 2006/2004 e capitolo 2 dell'allegato della decisione 2007/76/CE recante attuazione del regolamento CPC.

Quali informazioni possono essere incluse nel forum di discussione?

Il forum di discussione è annesso al CPCS ed è uno strumento destinato allo scambio di informazioni riguardanti questioni come i nuovi poteri di intervento e le migliori prassi. In generale il forum di discussione, anche se non è utilizzato frequentemente dagli agenti non dovrebbe servire per scambiare dati su casi particolari e non dovrebbe menzionare dati personali.

Quale tipo di dati possono essere inclusi nei sommari e nei documenti allegati?

La decisione 2007/76/CE recante attuazione del regolamento CPC prevede il campo di informazione «documenti allegati» nel caso di allarmi e richieste di informazione e di intervento. I sommari sono campi in cui va descritta un'infrazione. Si raccomanda di non inserire dati personali nei sommari poiché questi campi di informazioni sono riservati alla descrizione generale dell'infrazione. I dati personali figuranti nei documenti allegati che non sono strettamente necessari devono essere cancellati o eliminati.

Che cosa si intende per «ragionevole sospetto» di un'infrazione?

L'espressione «ragionevole sospetto» va interpretata facendo riferimento alle norme nazionali. Tuttavia, si raccomanda di inserire i sospetti di infrazione nel CPCS solo se esistono prove del fatto che l'infrazione è stata o potrebbe essere stata commessa.

Il trasferimento di dati verso paesi terzi

Il regolamento CPC [1] stabilisce che le informazioni comunicate nel quadro del regolamento CPC possono anche essere comunicate a un'autorità di un paese terzo da uno Stato membro che ha un accordo di assistenza bilaterale, a condizione che sia stato ottenuto il consenso dell'autorità competente che ha inizialmente comunicato l'informazione e che siano rispettate le disposizioni in materia di protezione dei dati.

In assenza di un accordo internazionale di cooperazione e assistenza reciproca tra l'Unione europea e un paese terzo [2], si raccomanda che qualsiasi accordo di assistenza bilaterale concluso con un dato paese terzo preveda adeguate garanzie di protezione dei dati e che sia notificato alle autorità competenti per la protezione dei dati, in modo che si possa procedere a un controllo preventivo, a meno che la Commissione ritenga che il paese terzo offre un livello adeguato di protezione dei dati personali trasferiti dall'Unione, in conformità all'articolo 25 della direttiva sulla protezione dei dati.

[1] Articolo 14, paragrafo 2, del regolamento CPC (CE) n. 2006/2004.
[2] Articolo 18 del regolamento CPC (CE) n. 2006/2004.