Consiglio dell'Unione europea

Bruxelles, 3 ottobre 2014
(OR. en)

13772/14

Fascicolo interistituzionale: 2012/0011 (COD)

DATAPROTECT 129
JAI 730
MI 726
DRS 120
DAPIX 137
FREMP 164
COMIX 503
CODEC 1926

NOTA

Origine:	presidenza
Destinatario:	Consiglio
n. doc. prec.:	13212/4/14 REV 4 DATAPROTECT 109 JAI 630 MI 579 DRS 104 DAPIX 109 FREMP 148 COMIX 403 CODEC 1675
Oggetto:	Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati) **[prima lettura]** - Capo IV

1. Il capo IV è stato ampiamente discusso in seno al Gruppo DAPIX nel primo semestre del 2013. Se alla riunione del Consiglio del 6-7 giugno 2013 tutte le delegazioni si sono congratulate con la presidenza irlandese per gli importantissimi progressi realizzati a tale riguardo, rimanevano tuttavia in sospeso diverse questioni, in particolare la necessità di ridurre ulteriormente gli oneri amministrativi/i costi di conformità derivanti da questo regolamento migliorando l'approccio basato sul rischio.

2. Durante la presidenza italiana il capo IV è stato ulteriormente discusso nelle riunioni del Gruppo DAPIX del 10-11 luglio e dell'11-12 settembre 2014. Le delegazioni hanno inoltre inviato osservazioni scritte[1]. Il capo IV è stato ulteriormente discusso nelle riunioni dei consiglieri GAI il 19, 22 e 29 settembre 2014, nonché nelle riunioni del Coreper del 25 settembre e del 1° ottobre 2014.

3. La presidenza vorrebbe esprimere la sua sincera gratitudine alle delegazioni per la cooperazione costruttiva che hanno dimostrato a tale riguardo. La presidenza è del parere che il risultato dei lavori sarà un riesame equilibrato del capo IV.

4. Alla luce di quanto precede la presidenza invita il Consiglio a raggiungere un orientamento generale parziale sul testo del capo IV che figura nell'allegato, sulla base dei seguenti presupposti:
   i. tale orientamento generale parziale deve essere raggiunto fermo restando che nulla è concordato finché tutto non è concordato e non esclude future modifiche al testo del capo IV per garantire la coerenza generale del regolamento;
   ii. tale orientamento generale parziale non pregiudica eventuali questioni orizzontali;
   iii. tale orientamento generale parziale non conferisce alla presidenza l'incarico di avviare triloghi informali sul testo con il Parlamento europeo.

---

[1] 12267/2/14 REV 2 DATAPROTECT 107 JAI 625 MI 574 DRS 102 DAPIX 107 FREMP 146 COMIX 395 CODEC 1671. L'Austria ha fatto circolare un contributo scritto: 13505/14 DATAPROTECT 124 JAI 700 MI 694 DRS 117 DAPIX 130 FREMP 159 COMIX 482 CODEC 1864.

(60) È opportuno stabilire la responsabilità generale del responsabile del trattamento per qualsiasi trattamento di dati personali che abbia effettuato direttamente o altri abbiano effettuato per suo conto. In particolare, il responsabile del trattamento dovrebbe (…) essere tenuto a mettere in atto opportune misure ed essere in grado di dimostrare la conformità delle (…) attività di trattamento con il presente regolamento (…). Tali misure dovrebbero tener conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

(60 *bis*) Tali rischi, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati suscettibili di cagionare un danno fisico, materiale o morale, in particolare se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati protetti da segreto professionale [violazione della (…) pseudonimia][2], o qualsiasi altro danno economico o sociale importante; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o dell'esercizio del controllo dei dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici o dati relativi alla salute o alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti della personalità, in particolare l'analisi e la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, lo stato di salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, per creare o utilizzare profili personali; se sono trattati dati personali di persone vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati; (…).

[2] Il riferimento all'utilizzo di dati pseudonimi al capo IV dovrà essere discusso in futuro nell'ambito di un ulteriore dibattito sulla pseudonimizzazione dei dati personali.

(60 *ter*) *La probabilità e la gravità del rischio dovrebbero essere determinate in funzione della natura, dell'oggetto, del contesto e delle finalità del trattamento dei dati. Il rischio dovrebbe essere considerato in base ad una valutazione oggettiva mediante cui si stabilisce se le operazioni di trattamento di dati comportano un rischio elevato. Un rischio elevato è un particolare*[3] *rischio di pregiudizio dei diritti e delle libertà delle persone fisiche* (…).

(60 *quater*) Gli orientamenti per la messa in atto di opportune misure e per dimostrare la conformità da parte del responsabile del trattamento [o dell'incaricato del trattamento], in particolare per quanto concerne l'individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, e l'individuazione di migliori prassi per attenuare il rischio, potrebbero essere forniti segnatamente da codici di condotta approvati, certificazioni approvate, linee direttrici del comitato europeo per la protezione dei dati o attraverso le indicazioni fornite da un responsabile della protezione dei dati. Il comitato europeo per la protezione dei dati può inoltre fornire orientamenti sulle operazioni di trattamento che si ritiene improbabile possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche e indicare quali misure possono essere sufficienti in questi casi per far fronte a tale rischio. (…)

(61) La tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento dei dati personali richiede l'attuazione di opportune misure tecniche ed organizzative onde garantire il rispetto delle disposizioni del presente regolamento. Al fine di essere in grado di dimostrare la conformità con il presente regolamento, il responsabile del trattamento dovrebbe adottare politiche interne e attuare misure adeguate, che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default. Tali misure potrebbero consistere, tra le altre cose, nel ridurre al minimo il trattamento dei dati personali, (…) pseudonimizzare i dati personali quanto prima, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al responsabile del trattamento di creare e migliorare caratteristiche di sicurezza. Quando si sviluppano, progettano, selezionano e utilizzano applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere la loro funzione, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i responsabili del trattamento e gli incaricati del trattamento possano adempiere ai loro obblighi di protezione dei dati.

---

[3] L'utilizzo del termine "particolare" è stato messo in discussione da BE, CZ, ES e UK, secondo cui tale termine non esprime la gravità del rischio in caso di rischio "elevato".

(62) La protezione dei diritti e delle libertà degli interessati così come la responsabilità generale dei responsabili del trattamento e **degli** incaricat**i** del trattamento, anche in relazione al monitoraggio e alle misure delle autorità di controllo, esigono una chiara attribuzione delle responsabilità ai sensi del presente regolamento, compresi i casi in cui un responsabile del trattamento stabilisca le finalità (…) e i mezzi del trattamento congiuntamente con altri responsabili del trattamento o quando l'operazione viene eseguita per conto del responsabile del trattamento.

(63) Quando un responsabile del trattamento non stabilito nell'Unione tratta dati personali di residenti nell'Unione e la sua attività di trattamento è finalizzata all'offerta di beni o alla prestazione di servizi a tali interessati o al controllo del loro comportamento nell'Unione, è opportuno che tale responsabile del trattamento designi un rappresentante, (…) *tranne se il trattamento da esso effettuato* **è occasionale ed è improbabile che** *presenti un rischio per i diritti e le libertà degli interessati, tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento*, **o se** il responsabile non è un'autorità pubblica o un organismo pubblico (…). Il rappresentante dovrebbe agire per conto del responsabile del trattamento e può essere interpellato da qualsiasi autorità di controllo. Il rappresentante dovrebbe essere esplicitamente autorizzato mediante mandato scritto del responsabile del trattamento ad agire a suo nome con riguardo agli obblighi che allo stesso derivano dal presente regolamento. La designazione di tale rappresentante non incide sulla responsabilità del responsabile del trattamento ai sensi del presente regolamento. Tale rappresentante dovrebbe svolgere i suoi compiti nel rispetto del mandato conferitogli dal responsabile del trattamento dei dati, anche per quanto concerne la cooperazione con le autorità di controllo competenti per qualsiasi misura adottata al fine di garantire il rispetto del presente regolamento. Il rappresentante designato dovrebbe essere oggetto di misure coercitive in caso di inadempienza da parte del responsabile del trattamento.

(63 *bis*) Per garantire che siano rispettate le prescrizioni del presente regolamento riguardo al trattamento che l'incaricato del trattamento deve eseguire per conto del responsabile del trattamento, quando affida delle attività di trattamento a un incaricato del trattamento, il responsabile del trattamento dovrebbe ricorrere unicamente a incaricati del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche ed organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento. (…) L'adesione dell'incaricato del trattamento ad un codice di condotta approvato o ad un meccanismo di certificazione approvato può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del responsabile del trattamento. L'esecuzione dei trattamenti su commissione dovrebbe essere disciplinata da un contratto o da altro atto giuridico a norma del diritto dell'Unione o dello Stato membro che vincoli l'incaricato del trattamento al responsabile del trattamento, in cui siano stipulati la materia disciplinata e la durata del trattamento, la natura e l**e** finalità del trattamento, il tipo di dati personali e le categorie di interessati, tenendo conto dei compiti e responsabilità specifici dell'incaricato del trattamento nel contesto del trattamento da eseguire e del rischio per i diritti e le libertà dell'interessato.

Il responsabile del trattamento e l'incaricato del trattamento possono scegliere di usare un contratto individuale o clausole contrattuali tipo che sono adottate o direttamente dalla Commissione o da un'autorità di controllo in conformità del meccanismo di coerenza e successivamente dalla Commissione, o che sono parte di una certificazione garantita nel meccanismo di certificazione. Dopo il completamento del trattamento per conto del responsabile del trattamento, l'incaricato del trattamento dovrebbe restituire o cancellare i dati personali salvo che il diritto dell'Unione o dello Stato membro cui è soggetto l'incaricato del trattamento preveda un requisito di conservazione dei dati.

(64) (…)

(65) Per dimostrare che si conforma al presente regolamento, il responsabile del trattamento o l'incaricato del trattamento dovrebbe tenere un registro di tutte le categorie di attività di trattamento effettuate sotto la sua responsabilità. Bisognerebbe obbligare tutti i responsabili del trattamento e gli incaricati del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possa servire per monitorare i trattamenti.

(66) Per mantenere la sicurezza e prevenire trattamenti contrari al presente regolamento, il responsabile del trattamento o l'incaricato del trattamento dovrebbe valutare il rischio (…) inerente al trattamento e provvedere a limitarlo. Tali provvedimenti dovrebbero assicurare un adeguato livello di sicurezza, compresa la riservatezza, tenuto conto della tecnologia disponibile e dei costi di (…) attuazione rispetto al rischio che presentano i trattamenti e alla natura dei dati da proteggere. (…). Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati, come la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso, in modo accidentale o illegale, a dati personali trasmessi, memorizzati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o morale.

(66 *bis*) Per migliorare il rispetto del presente regolamento nei casi in cui le operazioni di trattamento possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il responsabile del trattamento [o l'incaricato del trattamento] dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio. L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali è effettuato nel rispetto del presente regolamento. Laddove la valutazione d'impatto sulla protezione dei dati indica che le operazioni di trattamento presentano un rischio elevato che il responsabile del trattamento non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, prima del trattamento si dovrebbe consultare l'autorità di controllo.

(67) Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare (…) danni fisici, materiali o morali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei (…) loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie [violazione della (…) pseudonimia], pregiudizio alla reputazione, perdita di riservatezza dei dati protetti da segreto professionale o qualsiasi altro danno economico o sociale. (…). Pertanto, non appena viene a conoscenza di una violazione dei dati personali che (…) può provocare (…) danni fisici, materiali o morali, il responsabile del trattamento dovrebbe notificare la violazione all'autorità di controllo senza ingiustificato ritardo e, quando possibile, entro 72 ore. Oltre il termine di 72 ore, la notifica dovrebbe essere corredata di una giustificazione motivata. È opportuno che le persone fisiche i cui diritti e le cui libertà potrebbero essere gravemente compromessi da una siffatta violazione siano informate senza ingiustificato ritardo affinché possano prendere le precauzioni del caso. (…). La notifica dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. La notifica dovrebbe essere trasmessa non appena possibile, in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti (come le autorità incaricate dell'applicazione della legge). Ad esempio, (…) la necessità di attenuare un rischio immediato di danno richiederebbe che la notifica sia tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni ripetute o analoghe potrebbe giustificare tempi più lunghi.

(68) **(…)** Si deve verificare se sono state messe in atto tutte le opportune misure di protezione tecnologica ed organizzative per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato (…). È opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato. Siffatta notifica può dar luogo ad un intervento dell'autorità di controllo nell'ambito dei suoi poteri e funzioni previsti dal presente regolamento.

(68 *bis*) Non si dovrebbe richiedere la comunicazione di una violazione dei dati personali all'interessato se il responsabile del trattamento ha attuato le opportune misure tecnologiche di protezione e se tali misure sono state applicate ai dati personali oggetto della violazione. Tali misure tecnologiche di protezione dovrebbero includere quelle che rendono i dati incomprensibili a chiunque non sia autorizzato ad accedervi, in particolare criptando i dati personali (…).

(69) Nel definire modalità dettagliate relative al formato e alle procedure applicabili alla notifica delle violazioni di dati personali, è opportuno tenere debitamente conto delle circostanze della violazione, ad esempio stabilire se i dati personali fossero o meno protetti con opportuni dispositivi tecnici atti a limitare efficacemente il rischio di furto d'identità o altre forme di abuso. Inoltre, è opportuno che tali modalità e procedure tengano conto dei legittimi interessi delle autorità giudiziarie e di polizia, nei casi in cui una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di sicurezza.

(70) La direttiva 95/46/CE ha introdotto un obbligo generale di notificare alle autorità di controllo il trattamento dei dati personali. Tale obbligo comporta oneri amministrativi e finanziari senza per questo aver mai veramente contribuito a migliorare la protezione dei dati personali. È pertanto opportuno abolire tali obblighi generali e indiscriminati di notifica e sostituirli con meccanismi e procedure efficaci che si concentrino piuttosto su quei tipi di operazioni di trattamento che potenzialmente presentano un rischio elevato per i diritti e le libertà delle persone fisiche, per loro natura, oggetto, *contesto* e finalità (…). Questi tipi di operazioni di trattamento possono essere quelli che, in particolare, comportano l'utilizzo di nuove tecnologie o che sono di nuovo tipo e per i quali il responsabile del trattamento non ha effettuato preventivamente una valutazione d'impatto sulla protezione dei dati, o che si rivelano necessari alla luce del tempo trascorso dal trattamento iniziale[4].

[4] BE è contraria al riferimento temporale nell'ultima parte di questa frase.

(70 *bis*) In tali casi è opportuno che il responsabile del trattamento (…) effettui una valutazione d'impatto sulla protezione dei dati prima del trattamento, per valutare la particolare probabilità e gravità del rischio elevato, tenuto conto della natura, dell'oggetto, *del contesto* e delle finalità del trattamento e delle fonti di rischio, che verta in particolare anche sulle misure, sulle garanzie e sui meccanismi per attenuare tale rischio nonché per assicurare la protezione dei dati personali e per dimostrare la conformità al presente regolamento.

(71) Ciò dovrebbe applicarsi in particolare alle (…) operazioni di trattamento su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato, ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una nuova tecnologia su larga scala, nonché ad altre operazioni di trattamento che presentano un (…) rischio elevato per i diritti e le libertà degli interessati, specialmente nei casi in cui tali operazioni rendono più difficoltoso, per gli interessati, l'esercizio dei propri diritti. È opportuno altresì effettuare una valutazione d'impatto sulla protezione dei dati nei casi in cui i dati sono trattati per prendere decisioni riguardanti determinate persone fisiche in seguito a una valutazione sistematica e globale di aspetti della personalità delle persone fisiche, basata sulla profilazione di tali dati, o in seguito al trattamento di categorie particolari di dati personali, dati biometrici o dati relativi a condanne penali e reati o a connesse misure di sicurezza. Una valutazione d'impatto sulla protezione dei dati è altresì richiesta per la sorveglianza di zone accessibili al pubblico su larga scala, in particolare se effettuata mediante dispositivi ottico-elettronici, o per altri trattamenti che l'autorità di controllo competente ritiene possano presentare un rischio elevato per i diritti e le libertà degli interessati, specialmente perché impediscono a questi ultimi di esercitare un diritto o di avvalersi di un servizio o di un contratto, oppure perché sono effettuati sistematicamente su larga scala. *Il trattamento di (…) dati personali, indipendentemente dal volume o la natura dei dati, non dovrebbe essere considerato un trattamento su larga scala qualora sia tutelato dal segreto professionale (…), ad esempio il trattamento di dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario, ospedale o avvocato. In tali casi non dovrebbe essere obbligatorio procedere ad una valutazione d'impatto sulla protezione dei dati.*

(72) Vi sono circostanze in cui può essere ragionevole ed economico effettuare una valutazione d'impatto sulla protezione dei dati che verta su un oggetto più ampio di un unico progetto, per esempio quando autorità pubbliche o enti pubblici intendono istituire un'applicazione o una piattaforma di trattamento comuni o quando diversi responsabili del trattamento progettano di introdurre un'applicazione o un ambiente di trattamento comuni in un settore o segmento industriale o per una attività trasversale ampiamente utilizzata.

(73) Un'autorità pubblica o un ente pubblico possono procedere a una valutazione d'impatto sulla protezione dei dati se ciò non è già stato fatto in vista dell'adozione della legge nazionale che disciplina i compiti dell'autorità pubblica o dell'ente pubblico e lo specifico trattamento o insieme di trattamenti.

(74) Se dalla valutazione d'impatto sulla protezione dei dati risulta che il trattamento, nonostante le garanzie, le misure di sicurezza e i meccanismi previsti per attenuare il rischio, presenterebbe un rischio elevato per i diritti e le libertà delle persone fisiche (…) e il responsabile del trattamento è del parere che il rischio non possa essere ragionevolmente attenuato in termini di tecnologie disponibili e costi di attuazione, è opportuno consultare l'autorità di controllo prima dell'inizio delle attività di trattamento. Tale (…) rischio elevato potrebbe scaturire da certi tipi di trattamento di dati e da una certa estensione e frequenza del trattamento, da cui potrebbe derivare altresì (…) un danno o (…) un'interferenza con i diritti e le libertà dell'interessato. L'autorità di controllo che riceve una richiesta di consultazione dovrebbe darvi seguito entro un termine determinato. Tuttavia, la mancanza di reazione dell'autorità di controllo entro tale termine dovrebbe far salvo ogni intervento della stessa nell'ambito dei suoi poteri e funzioni previsti dal presente regolamento, compreso il potere di vietare le operazioni di trattamento. Nell'ambito di tale processo di consultazione, può essere presentato all'autorità di controllo il risultato di una valutazione d'impatto sulla protezione dei dati effettuata riguardo al trattamento in questione a norma dell'articolo 33, in particolare le misure previste per attenuare il rischio per i diritti e le libertà delle persone fisiche.

(74 *bis*) L'incaricato del trattamento, se necessario e su richiesta, dovrebbe assistere il responsabile del trattamento nel garantire il rispetto degli obblighi derivanti dallo svolgimento di una valutazione d'impatto sulla protezione dei dati e dalla previa consultazione dell'autorità di controllo.

(74 *ter*) L'autorità di controllo dovrebbe essere altresì consultata durante l'elaborazione di una misura legislativa o regolamentare che prevede il trattamento di dati personali (…) al fine di garantire che il trattamento previsto rispetti il presente regolamento e, in particolare, che si attenui il rischio per l'interessato.

(75) Per i trattamenti effettuati nel settore pubblico o per i trattamenti effettuati nel settore privato da una grande impresa o da un'impresa, a prescindere dalle sue dimensioni, le cui attività principali implicano operazioni di trattamento che richiedono un monitoraggio regolare e sistematico, il responsabile del trattamento o l'incaricato del trattamento può essere assistito da un'altra persona che ha una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto interno del presente regolamento. Tali "responsabili della protezione dei dati", dipendenti o meno del responsabile del trattamento, dovrebbero essere in grado di esercitare le loro funzioni e i loro compiti in maniera indipendente.

(76) Le associazioni o altre organizzazioni rappresentative dei responsabili del trattamento o degli incaricati del trattamento dovrebbero essere incoraggiate ad elaborare codici di condotta, nei limiti del presente regolamento, in modo da facilitarne l'effettiva applicazione, tenendo conto delle caratteristiche specifiche delle operazioni effettuate in alcuni settori e delle esigenze specifiche delle microimprese e delle piccole e medie imprese. In particolare, tali codici di condotta potrebbero calibrare gli obblighi dei responsabili del trattamento e degli incaricati del trattamento, tenuto conto del potenziale rischio del trattamento per i diritti e le libertà delle persone fisiche.

(76 *bis*) Nell'elaborare un codice di condotta, o nel modificare o nell'estendere tale codice, le associazioni e gli altri organismi rappresentanti le categorie di responsabili del trattamento o di incaricati del trattamento dovrebbero consultare le parti interessate pertinenti, compresi, quando possibile, gli interessati, e tener conto delle osservazioni ricevute e delle opinioni espresse in risposta a tali consultazioni.

(77) Al fine di migliorare la trasparenza e il rispetto del presente regolamento dovrebbe essere incoraggiata l'istituzione di meccanismi di certificazione, sigilli e marchi di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi.

CAPO IV

RESPONSABILE DEL TRATTAMENTO E INCARICATO DEL TRATTAMENTO[5]

SEZIONE 1
OBBLIGHI GENERALI

Articolo 22

Obblighi del responsabile del trattamento

1. Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità del rischio per i diritti e le libertà delle persone fisiche, il responsabile del trattamento (…) mette in atto opportune misure ed è in grado di dimostrare che il trattamento dei dati personali è effettuato conformemente al presente regolamento.

2. (…)

2 *bis*. Se ciò è proporzionato rispetto alle attività di trattamento[6], le misure di cui al paragrafo 1 includono l'attuazione di adeguate politiche in materia di protezione dei dati da parte del responsabile del trattamento.

2 *ter*. L'adesione a codici di condotta approvati, ai sensi dell'articolo 38, o un meccanismo di certificazione approvato, ai sensi dell'articolo 39, può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del responsabile del trattamento.

3. (…)

4. (…)

---

5 Riserva d'esame di SI e UK sull'intero capo. BE, DE, NL e UK non sono convinte delle cifre fornite dalla COM secondo cui la riduzione degli oneri amministrativi che pone fine all'obbligo generale di notifica per i responsabili del trattamento supera in valore gli ulteriori oneri amministrativi e costi di conformità derivanti dal regolamento proposto.

6 Secondo HU, RO e PL, questa formulazione concede troppo margine di manovra ai responsabili del trattamento. AT ritiene che, soprattutto per il rispetto dei limiti di tempo, il riferimento alla proporzionalità sia problematico.

Articolo 23

Protezione fin dalla progettazione e protezione di default

1. (…) Tenuto conto della tecnologia disponibile e dei costi di attuazione, nonché *della natura, dell'oggetto, del contesto e dell**e** finalità del trattamento*, come anche della probabilità e della gravità del rischio per i diritti e le libertà delle persone fisiche costituite dal trattamento, i responsabili del trattamento (…) mettono in atto misure tecniche e organizzative adeguate all'attività di trattamento in corso e ai suoi obiettivi, [incluse la minimizzazione e la pseudonimizzazione[7]], in modo tale che il trattamento soddisfi i requisiti del presente regolamento e tuteli i diritti (…) degli interessati.

2. Il responsabile del trattamento mette in atto opportune misure per garantire che siano trattati, di default, solo i dati personali (…) necessari[8] per ogni specifica finalità del trattamento; ciò vale per la quantità dei dati (…) raccolti, l'estensione del trattamento, il periodo di conservazione e la loro accessibilità. Quando il trattamento non è finalizzato a fornire informazioni al pubblico, detti meccanismi garantiscono che, di default, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento umano.

2 *bis*. Un meccanismo di certificazione approvato ai sensi dell'articolo 39 *può essere utilizzato come elemento* per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2.

3. (…)

4. (…)

---

[7] Secondo DE, in forza dell'articolo 5, lettera c), il principio dell'economia e della razionalizzazione dei dati, come pure l'anonimizzazione e la pseudonimizzazione, dovrebbero rientrare fra le opzioni chiave di attuazione. Questa discussione dovrà svolgersi tuttavia nel quadro di un dibattito sulla pseudonimizzazione dei dati personali.

[8] CZ preferirebbe "non eccessivi". Questo termine potrà essere cambiato nuovamente nel quadro del futuro dibattito sulla formulazione dell'articolo 5, paragrafo 1, lettera c).

Articolo 24

Corresponsabili del trattamento[9]

1. Allorché due o più responsabili del trattamento determinano congiuntamente le finalità e le modalità del trattamento dei dati personali, essi sono corresponsabili del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito al rispetto degli obblighi derivanti dal presente regolamento, con particolare riguardo (…) all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 14 e 14 *bis*, a meno che e nella misura in cui le rispettive responsabilità dei responsabili del trattamento siano determinate dal diritto dell'Unione o dello Stato membro cui essi sono soggetti. Tale accordo designa quale dei corresponsabili del trattamento fungerà da punto di contatto unico ai fini dell'esercizio da parte degli interessati dei loro diritti.

2. Indipendentemente dalle disposizioni dell'accordo di cui al paragrafo 1, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun responsabile del trattamento.

3. L'accordo riflette adeguatamente i rispettivi ed effettivi ruoli dei corresponsabili del trattamento e i loro rapporti con gli interessati, e il contenuto essenziale dell'accordo è messo a disposizione dell'interessato. Il paragrafo 2 non si applica qualora l'interessato sia stato informato in modo trasparente ed inequivocabile su chi sia responsabile tra i vari corresponsabili del trattamento, a meno che tale accordo diverso da quello determinato dal diritto dell'Unione o dello Stato membro non pregiudichi i diritti dell'interessato (…).

---

9 Riserva di SI, che ha messo in guardia contro potenziali conflitti giuridici in merito alla ripartizione delle responsabilità. SI ritiene pertanto che questo articolo debba essere ulteriormente riveduto nel contesto del futuro dibattito sul capo VIII. Anche FR ritiene che la ripartizione delle responsabilità tra il responsabile del trattamento e l'incaricato del trattamento sia molto vaga, mentre CZ ha sollevato dubbi in merito all'applicabilità di questa disposizione nel settore privato al di fuori di accordi presi all'interno di un gruppo di imprese: per la delegazione, tale disposizione dovrebbe contenere una garanzia contro l'esternalizzazione delle responsabilità.

Articolo 25

Rappresentanti di responsabili del trattamento non stabiliti nell'Unione

1. Ove si applichi l'articolo 3, paragrafo 2, il responsabile del trattamento designa per iscritto un rappresentante nell'Unione.

2. Quest'obbligo non si applica:

   (a) (…);

   (b) *al trattamento se quest'ultimo è* **occasionale**[10] **ed** *è improbabile che presenti un* (…) *rischio per i diritti e le libertà delle persone fisiche, tenuto conto della natura, del contesto, dell'oggetto e delle finalità del trattamento* (…);

   (c) alle autorità pubbliche o agli organismi pubblici;

   (d) (…).

3. Il rappresentante è stabilito in uno degli Stati membri in cui risiedono gli interessati i cui dati personali sono trattati nell'ambito dell'offerta di beni o servizi o il cui comportamento è controllato.

3 *bis*. Ai fini della conformità con il presente regolamento, il rappresentante è autorizzato dal responsabile del trattamento ad essere interpellato, in aggiunta o in sostituzione del responsabile del trattamento, in particolare dalle autorità di controllo e dagli interessati, per tutte le questioni riguardanti il trattamento di dati personali.

4. La designazione di un rappresentante a cura del responsabile del trattamento fa salve le azioni legali che potrebbero essere promosse contro lo stesso responsabile del trattamento.

---

10 Riserva di HU, SE e UK.

Articolo 26

Incaricato del trattamento

1. (…).[11] Il responsabile del trattamento ricorre unicamente a incaricati del trattamento che presentino garanzie sufficienti per mettere in atto opportune misure (…) tecniche ed organizzative in modo tale che il trattamento soddisfi i requisiti del presente regolamento (…).

1 *bis*. L'incaricato del trattamento non ricorre ad un altro incaricato senza il previo consenso specifico o generale per iscritto del responsabile del trattamento. In quest'ultimo caso l'incaricato del trattamento dovrebbe sempre informare il responsabile del trattamento di eventuali modifiche intenzionali riguardanti l'aggiunta o la sostituzione di altri incaricati del trattamento, dando così l'opportunità al responsabile del trattamento di obiettare a tali modifiche[12].

1 *ter*. (…)[13].

2. L'esecuzione dei trattamenti su commissione è disciplinata da un contratto o da altro atto giuridico a norma del diritto dell'Unione o di uno Stato membro che vincoli l'incaricato del trattamento al responsabile del trattamento, in cui sono stipulati la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati e i diritti del responsabile del trattamento (…), e che preveda in particolare che l'incaricato del trattamento:

   a) tratti i dati personali soltanto su istruzione del responsabile del trattamento (…), salvo che lo richieda il diritto dell'Unione o dello Stato membro cui è soggetto l'incaricato del trattamento; in tal caso, l'incaricato del trattamento informa il responsabile del trattamento circa tale obbligo giuridico prima del trattamento dei dati, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

---

11 La presidenza suggerisce di completare l'articolo 5, paragrafo 2, con l'espressione "anche nel caso di dati personali trattati a suo nome da parte di un incaricato del trattamento". Anche a tale riguardo possono essere necessarie ulteriori discussioni nel contesto del futuro dibattito sulla responsabilità nell'ambito del capo VIII.

12 LU e FI temono che ciò possa costituire un'interferenza indebita con la libertà contrattuale.

13 Alcune delegazioni (CZ, AT, LU) hanno segnalato la necessità di allineare questa disposizione all'articolo 77. La discussione sull'esercizio dei diritti degli interessati dovrebbe naturalmente svolgersi nel contesto del capo VIII.

b) (…)

c) prenda tutte le (…) misure richieste ai sensi dell'articolo 30;

d) rispetti le condizioni per ricorrere ad un altro incaricato del trattamento (…), come un requisito di autorizzazione preventiva specifica del responsabile del trattamento;

e) (…) tenuto conto della natura del trattamento, assista il responsabile del trattamento nel dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;

f) (…) assista il responsabile del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 30 a 34;

g) restituisca o cancelli, a scelta del responsabile del trattamento, i dati personali al cessare della prestazione dei servizi di trattamento di dati precisati nel contratto o altro atto giuridico, salvo che il diritto dell'Unione o dello Stato membro cui è soggetto l'incaricato del trattamento preveda un requisito di conservazione dei dati;

h) metta a disposizione del responsabile del trattamento (…) tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca agli audit realizzati dal responsabile del trattamento.

L'incaricato del trattamento informa immediatamente il responsabile del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o le disposizioni dell'Unione o dello Stato membro concernenti la protezione dei dati.

2 *bis*. Quando un incaricato del trattamento ricorre (…) ad un altro incaricato del trattamento per l'esecuzione di specifiche attività di trattamento per conto del responsabile del trattamento, su tale altro incaricato del trattamento sono imposti, *mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o dello Stato membro*[14], gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il responsabile del trattamento e l'incaricato del trattamento di cui al paragrafo 2, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro incaricato del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, l'incaricato iniziale conserva nei confronti del responsabile del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro incaricato.

2 bis bis. L'adesione dell'incaricato del trattamento ad un codice di condotta approvato, ai sensi dell'articolo 38, o un *meccanismo di certificazione* approvato, *ai sensi dell'articolo 39*[15], può essere utilizzata come elemento per dimostrare *le garanzie sufficienti di cui ai paragrafi 1 e 2 bis.*

2 *bis ter*. Fatto salvo un contratto individuale tra il responsabile del trattamento e l'incaricato del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 2 e 2 *bis* può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 2 *ter* e 2 *quater* o su clausole contrattuali tipo che sono parte di una certificazione concessa al responsabile del trattamento o all'incaricato del trattamento ai sensi degli articoli 39 e 39 *bis*.

---

14 HU ha suggerito di precisare questo riferimento al diritto dell'UE o degli SM aggiungendo "che vincoli l'altro incaricato del trattamento all'incaricato iniziale".

15 Riserva di FR; SK ha suggerito di specificare che, laddove l'altro incaricato del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati ai sensi di tale contratto o altro atto giuridico, l'incaricato del trattamento conserva nei confronti del responsabile del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro incaricato. Autorizzando l'incaricato del trattamento a "subcontrattarsi" e non obbligando il subincaricato del trattamento ad avere una relazione contrattuale con il responsabile del trattamento, si dovrebbe garantire al responsabile del trattamento sufficiente certezza giuridica in termini di responsabilità. Il principio della responsabilità dell'incaricato del trattamento principale in caso di violazioni del subincaricato è contemplato alla clausola 11 della decisione 2010/87/UE sulle clausole contrattuali tipo e nelle norme vincolanti d'impresa per gli incaricati del trattamento, ed è quindi lo standard attuale. È stato inoltre suggerito di sopprimere il riferimento all'articolo 2 *bis bis*.

2 *ter*. La Commissione può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 2 e 2 *bis* e in conformità della procedura d'esame di cui all'articolo 87, paragrafo 2[16].

2 *quater*. Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 2 e 2 *bis* in conformità del meccanismo di coerenza di cui all'articolo 57.

3. Il contratto o altro atto giuridico cui si fa riferimento ai paragrafi 2 e 2 *bis* sono tenuti in forma scritta, anche in formato elettronico.

4. (…)

5. (…)[17]

Articolo 27

Trattamento sotto l'autorità del responsabile del trattamento e dell'incaricato del trattamento

(…)

[16] PL ha espresso preoccupazione per l'eventualità che la Commissione non agisca. CY e FR si sono opposte al conferimento di questo ruolo alla COM (FR potrebbe forse accettarlo per il comitato europeo per la protezione dei dati).

[17] Riserva della COM sulla soppressione.

Articolo 28

Registri delle categorie di attività di trattamento dei dati personali[18]

1. Ogni responsabile del trattamento (…) ed eventuale rappresentante del responsabile del trattamento conserva un registro di tutte le categorie di attività di trattamento dei dati personali effettuate sotto la propria responsabilità. Il registro contiene (…) le seguenti informazioni:

   a) il nome e le coordinate di contatto del responsabile del trattamento, e di ogni corresponsabile del trattamento (…), del rappresentante del responsabile del trattamento ed eventualmente del responsabile della protezione dei dati;

   b) (…);

   c) le finalità del trattamento, compresi i legittimi interessi qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f);

   d) una descrizione delle categorie di interessati e delle pertinenti categorie di dati personali;

   e) (…) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare i destinatari di paesi terzi;

   f) se del caso, le categorie dei trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale (…);

   g) ove possibile, i termini ultimi previsti per cancellare le diverse categorie di dati;

   h) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 30, paragrafo 1.

18 Riserva d'esame di AT.

2 *bis*. Ciascun incaricato del trattamento tiene un registro delle categorie di attività di trattamento dei dati personali svolte per conto di un responsabile del trattamento, contenente:

a) nome e coordinate di contatto dell'incaricato o degli incaricati del trattamento, e di ogni responsabile del trattamento per conto del quale agisce l'incaricato del trattamento, e dell'eventuale rappresentante del responsabile del trattamento;

b) nome e coordinate di contatto dell'eventuale responsabile della protezione dei dati;

c) le categorie del trattamento effettuato per conto del responsabile del trattamento;

d) se del caso, le categorie dei trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;

e) ove possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative di cui all'articolo 30, paragrafo 1.

3 *bis*. I registri cui si fa riferimento ai paragrafi 1 e 2 *bis* sono tenuti in forma scritta, anche in formato elettronico o in qualunque altro formato non leggibile ma convertibile in un formato leggibile.

3. Su richiesta, il responsabile del trattamento, l'incaricato del trattamento e l'eventuale rappresentante del responsabile del trattamento mettono il registro (…) a disposizione dell'autorità di controllo.

4. Gli obblighi di cui ai paragrafi 1 e 2 *bis* non si applicano:

a) (…);

b) alle imprese o agli organismi con meno di 250 dipendenti, a meno che dai trattamenti che esse eseguono possa derivare un rischio elevato per i diritti e le libertà dell'interessato, (…) ad esempio discriminazione, furto o usurpazione d'identità, [violazione della (…) pseudonimia], perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati protetti da segreto professionale o qualsiasi altro danno economico o sociale agli interessati, tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento;

5. (…)

6. (…)

Articolo 29

Cooperazione con l'autorità di controllo

(…)

SEZIONE 2
SICUREZZA DEI DATI

Articolo 30

Sicurezza del trattamento

1. Tenuto conto della tecnologia disponibile e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche della probabilità e della gravità del rischio per i diritti e le libertà delle persone fisiche, il responsabile del trattamento e l'incaricato del trattamento mettono in atto opportune misure tecniche e organizzative [compresa **(…)** la pseudonimizzazione dei dati personali] per garantire un livello di sicurezza adeguato al rischio.

1 *bis*. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati da trattamenti di dati (…) derivanti in particolare dalla distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso, in modo accidentale o illegale, a dati personali trasmessi, memorizzati o comunque elaborati.

2. (…)

2 *bis*. L'adesione a codici di condotta approvati, ai sensi dell'articolo 38, o un meccanismo di certificazione approvato, ai sensi dell'articolo 39, può essere utilizzata come elemento per *dimostrare la conformità ai requisiti di cui al paragrafo 1*.

2 *ter*. Il responsabile del trattamento e l'incaricato del trattamento fanno sì che chiunque agisca sotto l'autorità del responsabile del trattamento o dell'incaricato del trattamento e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal responsabile del trattamento, salvo che lo richieda il diritto dell'Unione o di uno Stato membro.

3. (…)

4. (…)

Articolo 31

Notifica di una violazione dei dati personali all'autorità di controllo[19]

1. In caso di violazione dei dati personali suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, ad esempio discriminazione, furto o usurpazione d'identità, perdite finanziarie, [violazione della (…) pseudonimia], pregiudizio alla reputazione, perdita di riservatezza dei dati protetti da segreto professionale o qualsiasi altro danno economico o sociale importante, il responsabile del trattamento notifica la violazione all'autorità di controllo competente ai sensi dell'articolo 51 senza ritardo ingiustificato, ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza. Qualora non sia effettuata entro 72 ore, la notifica all'autorità di controllo è corredata di una giustificazione motivata.

1 *bis*. La notifica prevista al paragrafo 1 non è richiesta se, ai sensi dell'articolo 32, paragrafo 3, lettere a) e b), non è richiesta una comunicazione all'interessato[20].

2. (…) L'incaricato del trattamento informa il responsabile del trattamento senza ingiustificato ritardo dopo aver accertato la violazione dei dati personali.

---

19 Riserva d'esame di AT e SI. Riserva della COM: dovrebbe essere garantita la coerenza con il regime previsto dalla direttiva relativa alla vita privata e alle comunicazioni elettroniche; secondo SI, tale allineamento potrebbe essere realizzato eliminando l'aggettivo "elevato" quando si parla di "rischio" agli articoli 31 e 32.

20 BE, AT e PL ritengono che questo paragrafo debba essere soppresso.

3. La notifica di cui al paragrafo 1 deve come minimo:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile e appropriato, le categorie e il numero di interessati approssimativi in questione nonché le categorie e il numero approssimativo di registrazioni dei dati in questione;

b) indicare l'identità e le coordinate di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) (…)

d) descrivere le possibili conseguenze della violazione dei dati personali individuate dal responsabile del trattamento;

e) descrivere le misure adottate o di cui si propone l'adozione da parte del responsabile del trattamento per porre rimedio alla violazione dei dati personali; e

f) ove opportuno, indicare le misure intese ad attenuare i possibili effetti pregiudizievoli della violazione dei dati personali.

3 *bis*. Qualora e nella misura in cui non sia possibile fornire le informazioni di cui al paragrafo 3, lettere d), e) ed f), contestualmente alle informazioni di cui ai punti a) e b), il responsabile del trattamento trasmette dette informazioni senza ulteriore ingiustificato ritardo.

4. Il responsabile del trattamento documenta la violazione dei dati personali di cui ai paragrafi 1 e 2, incluse le circostanze in cui si è verificata, le sue conseguenze e i provvedimenti adottati per porvi rimedio. La documentazione deve consentire all'autorità di controllo di verificare il rispetto del presente articolo. (…).

5. (…)

6. (…)[21]

[21] Riserva della COM sulla soppressione.

Articolo 32

Comunicazione di una violazione dei dati personali all'interessato[22]

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, ad esempio discriminazione, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, [violazione della (…) pseudonimia], perdita di riservatezza dei dati protetti da segreto professionale o qualsiasi altro danno economico o sociale importante, il responsabile del trattamento (…) comunica la violazione all'interessato senza ingiustificato ritardo.

2. La comunicazione all'interessato di cui al paragrafo 1 descrive la natura della violazione dei dati personali e contiene almeno le informazioni e le raccomandazioni di cui all'articolo 31, paragrafo 3, lettere b), e) ed f).

3. Non è richiesta la comunicazione (…) all'interessato ai sensi del paragrafo 1 se:

   a. il responsabile del trattamento (…) ha utilizzato le opportune misure tecnologiche ed organizzative di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura; oppure

   b. il responsabile del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;

   c. detta comunicazione richiederebbe sforzi sproporzionati, in particolare a motivo del numero di casi in questione. In una simile circostanza, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia;

[22] Riserva d'esame di AT. Riserva della COM: dovrebbe essere garantita la coerenza con il regime previsto dalla direttiva relativa alla vita privata e alle comunicazioni elettroniche.

d. avrebbe ripercussioni negative su un interesse pubblico rilevante.

4. (…)

5. (…)

6. (…)[23]

SEZIONE 3

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI E CONSULTAZIONE PREVENTIVA

Articolo 33

Valutazione d'impatto sulla protezione dei dati [24]

1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato[25] per i diritti e le libertà delle persone fisiche, ad esempio discriminazione, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, [violazione della **(…)** pseudonimia], perdita di riservatezza dei dati protetti da segreto professionale o qualsiasi altro danno economico o sociale importante, il responsabile del trattamento (…)[26]effettua, prima di procedere al trattamento, una valutazione dell'impatto delle operazioni di trattamento previste sulla protezione dei dati personali. (…).

1 *bis*. Il responsabile del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, chiede un parere al responsabile della protezione dei dati, qualora ne sia designato uno.

---

23 Riserva della COM sulla soppressione.

24 FR, HU, AT e COM hanno espresso dubbi sul concetto di nuovi tipi di trattamento, che è ora chiarito al considerando 70. UK ritiene che tale obbligo non debba applicarsi laddove vi sia un interesse pubblico prevalente acciocché avvenga il trattamento (ad esempio un'emergenza sanitaria pubblica).

25 FR, RO, SK e UK hanno messo in guardia contro i notevoli oneri amministrativi derivanti dall'obbligo proposto. UK ritiene che qualsiasi requisito per procedere ad una valutazione d'impatto sulla protezione dei dati dovrebbe essere limitato ai casi in cui sussiste un rischio elevato identificato per i diritti degli interessati.

26 Riserva della COM sulla soppressione.

2. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei seguenti casi:

a) una valutazione sistematica e globale (…) di aspetti della personalità (…) degli interessati (…), basata sulla profilazione e da cui discendono decisioni[27] che hanno effetti giuridici sugli interessati o incidono gravemente sugli interessati;

b) il trattamento di categorie particolari di dati personali ai sensi dell'articolo 9, paragrafo 1 (…)[28], dati biometrici o dati relativi a condanne penali e reati o a connesse misure di sicurezza, qualora i dati siano trattati per prendere decisioni su larga scala riguardanti persone fisiche;

c) la sorveglianza di zone accessibili al pubblico *su larga scala*, in particolare se effettuata mediante dispositivi ottico-elettronici (…);

d) (…);

e) (…)[29].

2 *bis*. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di operazioni di trattamento soggette al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato europeo per la protezione dei dati. [30]

---

27 In futuro questa formulazione sarà allineata alla formulazione finale dell'articolo 20.

28 HU ha suggerito che i dati relativi ai minori siano altresì reinseriti.

29 Riserva d'esame di FR. PL ritiene opportuno affidare un ruolo al comitato europeo per la protezione dei dati al fine di determinare le operazioni a rischio elevato.

30 Riserva di CZ. HU si chiede quali eventuali conseguenze giuridiche potrebbero discendere da questo elenco delle tipologie di operazioni di trattamento redatto da un'autorità di protezione dei dati relativamente alle operazioni di trattamento in corso e quale sarebbe il relativo campo di applicazione territoriale. Secondo la presidenza, un eventuale ruolo del comitato europeo per la protezione dei dati a tale riguardo dovrebbe essere discusso nell'ambito del capo VII.

2 *ter*. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di operazioni di trattamento per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato europeo per la protezione dei dati.

2 *quater*. Prima di adottare gli elenchi di cui ai paragrafi 2 *bis* e 2 *ter*, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 57 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al controllo del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione. [31]

3. La valutazione contiene almeno una descrizione generale delle operazioni di trattamento previste, una valutazione del rischio di cui al paragrafo 1, le misure previste per affrontare il rischio, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e dei legittimi interessi degli interessati e delle altre persone in questione[32].

3 *bis*. Nella valutazione della liceità e dell'impatto del trattamento compiuto dai relativi responsabili o incaricati si tiene debito conto del rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 38, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati[33].

4. *Il responsabile del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto*, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza delle operazioni di trattamento (…)[34].

---

31 Riserva di CZ.
32 Riserva d'esame di FR.
33 Secondo HU, questo passaggio dovrebbe essere spostato in un considerando.
34 CZ e FR hanno indicato che si tratta di un obbligo del tutto irragionevole; riserva di IE.

5. (...) Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il responsabile del trattamento è soggetto un fondamento giuridico attraverso un atto legislativo che disciplina l'operazione di trattamento specifica o l'insieme di operazioni in questione[35], i paragrafi 1, 2 e 3 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

6. (…)

7. (…)

Articolo 34

(…) Consultazione preventiva[36]

1. (…)

2. Il responsabile del trattamento (…)[37], prima di procedere al trattamento dei dati personali, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati di cui all'articolo 33 indichi che il trattamento presenterebbe un (…) rischio elevato in assenza di misure che *il responsabile del trattamento dovrebbe adottare* per attenuare il rischio.

---

35 BE e SI hanno indicato che questo passaggio dovrà essere riesaminato nel contesto del futuro dibattito su come includere il settore pubblico nel campo di applicazione del regolamento.

36 Riserva d'esame di HU; riserva di SK sul fatto di attribuire questo ruolo ad autorità di protezione dei dati, le quali potrebbero non essere in grado di occuparsi di tali consultazioni nella totalità dei casi. ES ha proposto di esonerare i responsabili del trattamento dall'obbligo di consultazione preventiva qualora abbiano nominato un RPD.

37 Riserva di COM e LU sulla soppressione dell'incaricato del trattamento.

3. Se ritiene che il trattamento previsto di cui al paragrafo 2 non sia conforme al presente regolamento, in particolare qualora il responsabile del trattamento non abbia identificato o attenuato sufficientemente *il rischio*, l'autorità di controllo, entro un periodo massimo di sei settimane dalla richiesta di consultazione, fornisce una consulenza al responsabile del trattamento dei dati, per iscritto, e può avvalersi dei poteri di cui[38] all'articolo 53 (…). Questo periodo può essere prorogato di ulteriori sei settimane, tenendo conto della complessità del trattamento previsto. Qualora si applichi la proroga, il responsabile del trattamento o l'incaricato del trattamento è informato entro un mese dal ricevimento della richiesta sui motivi del ritardo.

4. (…)

5. (…)

6. Al momento di consultare l'autorità di controllo ai sensi del paragrafo 2, il responsabile del trattamento (…) trasmette all'autorità di controllo:

   a) se del caso, le rispettive responsabilità del responsabile del trattamento, dei corresponsabili e coincaricati del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo di imprese;

   b) le finalità e i mezzi del trattamento previsto;

   c) le misure e le garanzie previste per tutelare i diritti e le libertà degli interessati a norma del presente regolamento;

   d) se del caso, le coordinate di contatto del responsabile della protezione dei dati;

   e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 33;

   f) ogni (…) altra informazione richiesta dall'autorità di controllo (…).

---

38 Riserva di UK, che ritiene che il potere di vietare le operazioni di trattamento non debba applicarsi in periodi in cui vi sia un interesse pubblico prevalente acciocché avvenga il trattamento (ad esempio un'emergenza sanitaria pubblica). La presidenza ritiene che questa questione debba comunque essere discussa nel contesto del capo VI sui poteri dell'autorità di protezione dei dati, poiché questi possono ovviamente essere utilizzati anche indipendentemente da eventuali consultazioni.

7. Gli Stati membri consultano l'autorità di controllo durante l'elaborazione di una proposta di misura legislativa adottata dai parlamenti nazionali o di misura regolamentare basata su detto atto legislativo che preveda il trattamento di dati personali (…)[39].

7 *bis*. In deroga al paragrafo 2, il diritto degli Stati membri può richiedere che i responsabili del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento di dati personali da parte di un responsabile del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento dei dati con riguardo alla protezione sociale e alla pubblica sanità[40].

8. (…)

9. (…)

[39] Riserva d'esame di IE sulla soppressione.
[40] Riserva d'esame di SE.

SEZIONE 4
RESPONSABILE DELLA PROTEZIONE DEI DATI

Articolo 35

Designazione del responsabile della protezione dei dati

1. Il responsabile del trattamento o l'incaricato del trattamento possono designare o, se previsto dal diritto dell'Unione o degli Stati membri, designano[41](…) un responsabile della protezione dei dati.

2. Un gruppo di imprese può nominare un unico responsabile della protezione dei dati.

3. Qualora il responsabile del trattamento o l'incaricato del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

4. (…).

5. Il (…) responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati, e della capacità di adempiere ai compiti di cui all'articolo 37, in particolare l'assenza di conflitto di interessi. (…).

6. (…)

7. (…). Durante il mandato il responsabile della protezione dei dati può essere destituito, oltre che per gravi motivi i quali, a norma del diritto dello Stato membro interessato, giustifichino la destituzione di un dipendente o di un funzionario pubblico, solo se non soddisfa più le condizioni richieste per l'esercizio delle sue funzioni a norma dell'articolo 37.

---

41 Reso opzionale a seguito di una decisione del Consiglio. Riserva d'esame di AT. DE, HU e AT avrebbero preferito definire i casi di nomina obbligatoria dell'autorità di protezione dei dati nel regolamento stesso e potrebbero voler tornare su questo punto in un secondo tempo. Riserva della COM sulla natura facoltativa e sulla soppressione delle lettere a), b) e c).

8. Il responsabile della protezione dei dati può essere un membro del personale del responsabile del trattamento o dell'incaricato del trattamento oppure adempiere ai suoi compiti in base a un contratto di servizi.

9. Il responsabile del trattamento o l'incaricato del trattamento pubblica le coordinate di contatto del responsabile della protezione dei dati e le comunica all'autorità di controllo (…).

10. Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti riconosciuti dal presente regolamento.

11. (…)

Articolo 36

Posizione del responsabile della protezione dei dati

1. Il responsabile del trattamento o l'incaricato del trattamento si assicura che il responsabile della protezione dei dati sia prontamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

2. Il responsabile del trattamento o l'incaricato del trattamento sostiene il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 37 fornendogli (…) le risorse necessarie per adempiere a tali compiti nonché l'accesso ai dati personali e alle operazioni di trattamento.

3. Il responsabile del trattamento o l'incaricato del trattamento si assicura che il responsabile della protezione dei dati possa agire in maniera indipendente nell'adempimento dei propri compiti e non riceva alcuna istruzione per quanto riguarda il loro esercizio. Il responsabile della protezione dei dati non è penalizzato dal responsabile del trattamento o dall'incaricato del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente ai massimi superiori gerarchici del responsabile del trattamento o dell'incaricato del trattamento.

4. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il responsabile del trattamento o l'incaricato del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

Articolo 37

Compiti del responsabile della protezione dei dati

1. Il (…) responsabile della protezione dei dati è (...) incaricato delle seguenti funzioni:

a) informare e consigliare il responsabile del trattamento o l'incaricato del trattamento nonché i dipendenti che trattano dati personali in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati(…);

b) sorvegliare l'osservanza del presente regolamento, delle altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del responsabile del trattamento o dell'incaricato del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e gli audit connessi;

c) (…)

d) (…)

e) (…)

f) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 33;

g) controllare che sia dato seguito alle richieste dell'autorità di controllo e, nell'ambito delle sue competenze, cooperare con l'autorità di controllo di propria iniziativa o su sua richiesta;

h) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento di dati personali, tra cui la consultazione preventiva di cui all'articolo 34 e, se del caso, effettuare consultazioni su qualunque altra questione.

2. (…)

2 bis. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della *natura, dell'oggetto, del contesto e delle finalità* del trattamento.

SEZIONE 5
CODICI DI CONDOTTA E CERTIFICAZIONE

Articolo 38

Codici di condotta[42]

1. Gli Stati membri, le autorità di controllo, il comitato europeo per la protezione dei dati e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità settoriali e delle esigenze specifiche delle micro, piccole e medie imprese.

1 *bis*. Le associazioni e gli altri organismi rappresentanti le categorie di responsabili del trattamento o incaricati del trattamento possono elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione delle disposizioni del presente regolamento, ad esempio:

a) il trattamento equo e trasparente dei dati;

a bis) i legittimi interessi perseguiti dal responsabile del trattamento in contesti specifici;

b) la raccolta dei dati;

b bis) la pseudonimizzazione dei dati personali;

c) l'informazione del pubblico e dell'interessato;

d) l'esercizio dei diritti degli interessati;

e) l'informazione e la protezione del minore e il modo in cui è ottenuto il consenso del genitore e del tutore;

e bis) le misure e le procedure di cui agli articoli 22 e 23 e le misure volte a garantire la sicurezza del trattamento di cui all'articolo 30;

---

[42] Riserva d'esame di AT, FI, SK e PL.

e ter) la notificazione di una violazione dei dati personali alle autorità di controllo e la comunicazione di detta violazione all'interessato;

f) (…).

1 bis ter. Oltre ai responsabili del trattamento o agli incaricati del trattamento soggetti al presente regolamento, possono conformarsi ai codici di condotta *approvati* ai sensi del paragrafo 2 anche i responsabili del trattamento o gli incaricati del trattamento non soggetti al presente regolamento ai sensi dell'articolo 3, al fine di fornire adeguate garanzie nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali alle condizioni di cui all'articolo 42, paragrafo 2, lettera d). Detti responsabili del trattamento o incaricati del trattamento assumono l'impegno vincolante ed esecutivo, mediante strumenti contrattuali o di altro genere, di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati.

1 ter. Il codice di condotta contiene i meccanismi che consentono all'organismo di cui all'articolo 38 bis, paragrafo 1, di effettuare il controllo obbligatorio[43] del rispetto delle norme del codice da parte dei responsabili del trattamento o degli incaricati del trattamento che si impegnano ad aderirvi, fatti salvi le funzioni e i poteri dell'autorità di controllo competente ai sensi degli articoli 51 o 51 bis .

2. Le associazioni e gli altri organismi di cui al paragrafo 1 bis che intendono preparare un codice di condotta o modificare o prorogare un codice di condotta esistente, sottopongono il progetto di codice all'autorità di controllo competente ai sensi dell'articolo 51. L'autorità di controllo esprime un parere sulla conformità al presente regolamento del progetto di codice di condotta o della modifica o della proroga proposta e lo approva, lo modifica o lo proroga se ritiene che offra garanzie sufficientemente adeguate.

2 bis. Qualora il parere, di cui al paragrafo 2, confermi che il codice di condotta o il codice modificato o prorogato è conforme al presente regolamento e viene quindi approvato, e se il codice stesso non si riferisce alle attività di trattamento in vari Stati membri, l'autorità di controllo registra il codice e ne pubblica le relative specifiche.

[43] CZ preferisce che tale controllo sia facoltativo.

2 ter. Qualora il codice progetto di condotta si riferisca alle attività di trattamento in vari Stati membri, prima di approvarlo l'autorità di controllo competente ai sensi dell'articolo 51 lo sottopone, tramite la procedura di cui all'articolo 57, al comitato europeo per la protezione dei dati il quale formula un parere sulla conformità del progetto di codice, o sul codice modificato o prorogato al presente regolamento o, nel caso di cui al paragrafo 1 bis ter, sulla previsione di adeguate garanzie[44].

3. Qualora il parere di cui al paragrafo 2 ter confermi che il codice di condotta o il codice modificato o prorogato è conforme al presente regolamento o, nel caso di cui al paragrafo 1 bis ter, che fornisce adeguate garanzie, il comitato europeo per la protezione dei dati trasmette il suo parere alla Commissione.

4. La Commissione può decidere con atto di esecuzione che i codici di condotta approvati e le modifiche o proroghe dei codici di condotta approvati esistenti che le sono stati sottoposti ai sensi del paragrafo 3 hanno validità generale all'interno dell'Unione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 87, paragrafo 2.

5. La Commissione provvede ad un'appropriata divulgazione dei codici approvati per i quali è stata decisa la validità generale ai sensi del paragrafo 4.

5 bis. Il comitato europeo per la protezione dei dati raccoglie in un registro tutti i codici di condotta approvati e le relative modifiche e li rende pubblici con qualsiasi mezzo appropriato, ad esempio tramite il portale europeo della giustizia elettronica.

[44] FR ha proposto il seguente paragrafo 2 quater: "I codici di condotta approvati ai sensi del paragrafo 2 bis costituiscono un elemento della relazione contrattuale tra il responsabile del trattamento e l'interessato. Se detti codici di condotta determinano la conformità del responsabile del trattamento o dell'incaricato del trattamento al presente regolamento, essi sono giuridicamente vincolanti ed esecutivi."

Articolo 38 bis

Controllo dei codici di condotta approvati[45]

1. Fatti salvi le funzioni e i poteri dell'autorità di controllo competente, di cui agli articoli 52 e 53, il controllo della conformità con un codice di condotta ai sensi dell'articolo 38, paragrafo 1 ter, può essere effettuato da un organismo[46] in possesso del livello adeguato di competenze riguardo al contenuto del codice e del necessario accreditamento a tal fine dell'autorità di controllo competente.

2. L'organismo di cui al paragrafo 1 può essere accreditato a tal fine se:

   a) riguardo al contenuto del codice ha dimostrato in modo convincente alla competente autorità di controllo di essere indipendente e competente;

   b) ha istituito procedure che gli consentono di valutare l'ammissibilità dei responsabili del trattamento e degli incaricati del trattamento in questione ad applicare il codice, di controllare che detti responsabili e incaricati ne rispettino le disposizioni e di riesaminarne periodicamente il funzionamento;

   c) ha istituito procedure e strutture atte a trattare i reclami concernenti violazioni del codice o il modo in cui il codice è stato o è attuato da un responsabile del trattamento o un incaricato del trattamento ed ha gli strumenti necessari a rendere dette procedure e strutture trasparenti per gli interessati e il pubblico;

   d) dimostra in modo convincente per l'autorità di controllo competente che i compiti e le funzioni da esso svolti non danno adito a conflitto di interessi.

---

45 Riserva d'esame di AT e LU.

46 CZ, ES e LU sono contrarie ad affidare questo compito a tali organismi separati. Tra le altre preoccupazioni, è stato evocato l'onere amministrativo connesso alla creazione di detti organismi. I codici di condotta sono un meccanismo completamente volontario al quale nessun responsabile del trattamento è obbligato a partecipare.

3. L'autorità di controllo competente presenta al comitato europeo per la protezione dei dati il progetto di criteri per l'accreditamento dell'organismo di cui al paragrafo 1, ai sensi del meccanismo di coerenza di cui all'articolo 57.

4. Fatte salve le disposizioni del capo VIII, un organismo di cui al paragrafo 1 può prendere, stanti adeguate garanzie, le opportune misure in caso di violazione del codice da parte di un responsabile del trattamento o incaricato del trattamento, tra cui la sospensione o l'esclusione dal codice del responsabile del trattamento o dell'incaricato del trattamento. Esso informa l'autorità di controllo competente di tali misure e dei motivi della loro adozione.

5. L'autorità di controllo competente revoca l'accreditamento dell'organismo, di cui al paragrafo 1, se le condizioni per l'accreditamento non sono, o non sono più, rispettate o se le misure adottate dall'organismo non sono conformi al presente regolamento.

6. Il presente articolo non si applica al trattamento di dati personali effettuato da autorità pubbliche e da organismi pubblici.

Articolo 39

Certificazione[47]

1. Gli Stati membri, il comitato europeo per la protezione dei dati e la Commissione incoraggiano, in particolare a livello unionale, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento delle operazioni di trattamento effettuate dai responsabili del trattamento e dagli incaricati del trattamento. Si tiene conto delle esigenze specifiche delle micro, piccole e medie imprese.

[47] Riserva d'esame di AT, FR e FI. FR ritiene che la terminologia utilizzata sia poco chiara e che l'autorità di protezione dei dati debba essere in grado di controllare la conformità alle politiche in materia di protezione dei dati; quest'ultimo punto va chiarito nell'articolo 53.

1 bis. I meccanismi, i sigilli e i marchi *approvati* ai sensi del paragrafo 2 bis, oltre ad essere stabiliti affinché vengano applicati dai responsabili del trattamento e dagli incaricati del trattamento soggetti al presente regolamento, possono essere stabiliti anche al fine di dimostrare la previsione di adeguate garanzie da parte dei responsabili del trattamento o incaricati del trattamento non soggetti al presente regolamento ai sensi dell'articolo 3, nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali alle condizioni di cui all'articolo 42, paragrafo 2, lettera e). Detti responsabili del trattamento o incaricati del trattamento assumono l'impegno vincolante ed esecutivo, mediante strumenti contrattuali o di altro genere, di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati.

2. La certificazione ai sensi del presente articolo non riduce la responsabilità del responsabile del trattamento o dell'incaricato del trattamento riguardo alla conformità al presente regolamento e lascia impregiudicati le funzioni e i poteri dell'autorità di controllo competente a norma dell'articolo 51 o 51 bis .

2 bis. La certificazione ai sensi del presente articolo è rilasciata dagli *organismi di* certificazione *di cui all'articolo 39 bis o, se del caso, da parte dell'autorità di controllo competente* in base ai criteri approvati dall'autorità di controllo competente o, *ai sensi dell'articolo 57*, dal comitato europeo per la protezione dei dati[48].

3. Il responsabile del trattamento o l'incaricato del trattamento che sottopone il trattamento effettuato al meccanismo di certificazione trasmette all'organismo di certificazione previsto all'articolo 39 bis *o, se del caso, all'autorità di controllo competente* tutte le informazioni e gli consente l'accesso alle attività di trattamento necessarie a espletare la procedura di certificazione.

4. La certificazione viene rilasciata al responsabile del trattamento o incaricato del trattamento per un periodo massimo di 3 anni e può essere rinnovata alle stesse condizioni purché continuino ad essere soddisfatti i requisiti pertinenti. Viene revocata dagli organismi di certificazione di cui all'articolo 39 bis o, se del caso, dall'autorità di controllo competente, qualora non siano o non siano più soddisfatte i requisiti pertinenti.

---

48 Ciò lascia impregiudicata la futura discussione sugli esatti poteri del comitato europeo per la protezione dei dati, che saranno trattati nel contesto della discussione sul meccanismo di sportello unico.

5. Il comitato europeo per la protezione dei dati raccoglie in un registro tutti i meccanismi di certificazione e i sigilli di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato, ad esempio tramite il portale europeo della giustizia elettronica.

Articolo 39 bis

Organismo di certificazione e relativa procedura[49]

1. Fatti salvi le funzioni e i poteri dell'autorità di controllo competente, di cui agli articoli 52 e 53, la certificazione viene rilasciata e rinnovata da un organismo di certificazione in possesso del livello adeguato di competenze riguardo alla protezione dei dati. Ogni Stato membro stabilisce se tali organismi di certificazione siano accreditati[50]:

   a) dall'autorità di controllo competente ai sensi dell'articolo 51 o 51 bis, e/o

   b) dall'organismo nazionale di accreditamento designato in virtù del regolamento (CE) 765/2008 del Parlamento europeo e del Consiglio che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti conformemente alla norma EN-ISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'autorità controllo competente ai sensi dell'articolo 51 o 51 bis.

2. L'organismo di certificazione di cui al paragrafo 1 può essere accreditato a tal fine solo se:

   a) riguardo al contenuto della certificazione ha dimostrato in modo convincente alla competente autorità di controllo di essere indipendente e competente;

[49] Riserva d'esame di AT, FR e LU.
[50] Riserva d'esame di BE.

a bis) si è impegnato a rispettare i criteri *di cui al paragrafo 2 bis dell'articolo 39* e approvati dall'autorità di controllo competente ai sensi dell'articolo 51 o 51 bis o, ai sensi dell'articolo 57, dal comitato europeo di protezione dei dati;

b) ha istituito procedure per il rilascio, il riesame periodico e il ritiro dei sigilli e dei marchi di protezione dei dati;

c) ha istituito procedure e strutture atte a trattare i reclami concernenti violazioni della certificazione o il modo in cui la certificazione è stata o è attuata dal responsabile del trattamento o dall'incaricato del trattamento ed ha gli strumenti necessari a rendere dette procedure e strutture trasparenti per gli interessati e il pubblico;

d) dimostra in modo convincente per l'autorità di controllo competente che i compiti e le funzioni da esso svolti non danno adito a conflitto di interessi.

3. L'accreditamento degli organi di certificazione di cui al paragrafo 1 ha luogo in base ai criteri approvati dall'autorità di controllo competente ai sensi dell'articolo 51 o 51 bis o, *ai sensi dell'articolo 57*, dal comitato europeo di protezione dei dati[51]. *In caso di accreditamento ai sensi del paragrafo 1, lettera b), tali requisiti integrano quelli previsti dal regolamento 765/2008 nonché le norme tecniche che definiscono i metodi e le procedure degli organismi di certificazione.*

4. L'organismo di certificazione di cui al paragrafo 1 è responsabile della corretta valutazione che comporta la certificazione o la revoca di quest'ultima, fatta salva la responsabilità del responsabile del trattamento o dell'incaricato del trattamento riguardo alla conformità al presente regolamento. L'accreditamento è rilasciato per un periodo massimo di 5 anni e può essere rinnovato alle stesse condizioni purché l'organismo soddisfi i requisiti.

5. L'organismo di certificazione di cui al paragrafo 1 trasmette all'autorità di controllo competente i motivi del rilascio o della revoca della certificazione richiesta.

---

51 Ciò lascia impregiudicata la futura discussione sugli esatti poteri del comitato europeo per la protezione dei dati, che saranno trattati nel contesto della discussione sul meccanismo di sportello unico.

6. I requisiti di cui al paragrafo 3 e i criteri di cui al paragrafo 2 bis dell'articolo 39 *sono resi pubblici dall'autorità di controllo in forma facilmente accessibile*. Le autorità di controllo provvedono a trasmetterli anche al comitato europeo per la protezione dei dati. Il comitato europeo per la protezione dei dati raccoglie in un registro tutti i meccanismi di certificazione e i sigilli di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato, ad esempio tramite il portale europeo della giustizia elettronica.

6 bis. Fatte salve le disposizioni del capo VIII, l'autorità di controllo competente o l'organismo nazionale di accreditamento revoca l'accreditamento rilasciato all'organismo di certificazione, di cui al paragrafo 1, se le condizioni per l'accreditamento non sono, o non sono più, rispettate o se le misure adottate dall'organismo non sono conformi al presente regolamento[52].

7. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 86, al fine di (...) precisare i criteri e i requisiti di cui occorre tener conto per i meccanismi di certificazione della protezione dei dati di cui al paragrafo 1, [comprese le condizioni di rilascio e revoca e i requisiti per il riconoscimento della certificazione e i requisiti relativi a un modello di "sigillo europeo per la protezione dei dati" nell'Unione e in paesi terzi].

7 bis. Il comitato europeo per la protezione dei dati fornisce alla Commissione pareri sui criteri e i requisiti di cui al paragrafo 7[53].

8. La Commissione può stabilire norme tecniche riguardanti i meccanismi di certificazione e i sigilli e marchi di protezione dei dati e le modalità per promuovere e riconoscere i meccanismi di certificazione e i sigilli e marchi di protezione dei dati. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 87, paragrafo 2[54].

---

52 CZ, FR e HU ritengono che l'organismo nazionale di accreditamento debba sempre consultare il comitato europeo per la protezione dei dati prima di accreditare un organismo di certificazione.

53 Ciò lascia impregiudicata la futura discussione sugli esatti poteri del comitato europeo per la protezione dei dati, che saranno trattati nel contesto della discussione sul meccanismo di sportello unico.

54 DE ha chiesto di sopprimere gli ultimi due paragrafi e ha suggerito di aggiungere un nuovo paragrafo: "I paragrafi precedenti lasciano impregiudicate le norme che disciplinano la responsabilità degli organismi di certificazione nazionali, le procedure di accreditamento e la specificazione dei criteri per la sicurezza e la protezione dei dati. Il potere della Commissione di adottare atti delegati ai sensi dei paragrafi 7 e 8 non si applica alle procedure di certificazione nazionali e internazionali effettuate su tale base. I certificati di sicurezza rilasciati dagli organismi competenti o da organismi da questi ultimi accreditati nel quadro di dette procedure sono reciprocamente riconosciuti." Anche ES ritiene che questa competenza non vada lasciata esclusivamente alla Commissione.