COMMISSIONE
EUROPEA

Bruxelles, 24.1.2018
COM(2018) 43 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

Maggiore protezione, nuove opportunità – Orientamenti della Commissione per l'applicazione diretta del regolamento generale sulla protezione dei dati a partire dal 25 maggio 2018

Comunicazione della Commissione al Parlamento europeo e al Consiglio

Maggiore protezione, nuove opportunità – Orientamenti della Commissione per l'applicazione diretta del regolamento generale sulla protezione dei dati a partire dal 25 maggio 2018

Introduzione

Il 6 aprile 2016 l'Unione europea ha deciso di modificare radicalmente il quadro giuridico relativo alla protezione dei dati adottando il pacchetto di riforma in materia comprendente il regolamento generale sulla protezione dei dati[1] ("regolamento"), che sostituisce la ventennale direttiva 95/46/CE[2] ("direttiva sulla protezione dei dati"), e la direttiva sulla protezione dei dati nell'ambito della cooperazione giudiziaria e di polizia[3]. Il regolamento, nuovo strumento di protezione dei dati a livello di Unione, diventerà direttamente applicabile il 25 maggio 2018, due anni dopo la sua adozione ed entrata in vigore[4].

Il regolamento rafforzerà la tutela del diritto dei cittadini alla protezione dei dati personali, riflettendone la natura di diritto fondamentale dell'Unione europea[5].

Prevedendo un unico insieme di norme direttamente applicabili negli ordinamenti giuridici degli Stati membri, garantirà la libera circolazione dei dati personali tra gli Stati membri dell'UE e rafforzerà la fiducia e la sicurezza dei consumatori, due elementi indispensabili per un vero mercato unico digitale. Il regolamento creerà così nuove opportunità per le attività commerciali e le imprese, soprattutto quelle di piccole dimensioni, anche chiarendo le norme relative al trasferimento internazionale di dati.

Pur basandosi sulla normativa vigente, il nuovo quadro giuridico avrà effetti di ampia portata e, sotto alcuni aspetti, richiederà notevoli adeguamenti. Per questo motivo, il regolamento prevede un periodo di transizione di due anni – fino al 25 maggio 2018 – per offrire agli Stati membri e alle parti interessate il tempo di prepararsi ad applicare pienamente il nuovo quadro giuridico.

Nel corso degli ultimi due anni tutte le parti interessate, dalle amministrazioni nazionali e autorità nazionali di protezione dei dati ai titolari del trattamento e responsabili del trattamento, hanno intrapreso varie attività per assicurare che l'importanza e l'ampiezza dei cambiamenti introdotti dalle nuove disposizioni in materia di protezione dei dati siano ben

---

1 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016).

2 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 (GU L 281 del 23.11.1995).

3 Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119 del 4.5.2016).

4 Il regolamento è in vigore dal 24 maggio 2016 e si applica a decorrere dal 25 maggio 2018.

5 Articolo 8 della Carta dei diritti fondamentali dell'Unione europea e articolo 16 del TFUE.

chiare e tutti i soggetti interessati siano pronti ad applicarle. Con l'avvicinarsi della scadenza del 25 maggio, la Commissione ritiene necessario fare il punto delle attività svolte e valutare eventuali altri provvedimenti che potrebbero essere utili per garantire che tutto sia pronto per la riuscita applicazione del nuovo quadro giuridico[6].

La presente comunicazione:

- riepiloga le principali novità e opportunità offerte dalla nuova normativa dell'UE in materia di protezione dei dati;
- fa il punto delle attività preparatorie svolte finora a livello di Unione;
- delinea ciò che la Commissione europea, le autorità nazionali di protezione dei dati e le amministrazioni nazionali devono ancora compiere per portare a termine con successo i preparativi;
- indica le misure che la Commissione intende adottare nei prossimi mesi.

Inoltre, parallelamente all'adozione della presente comunicazione, la Commissione vara uno strumentario online per aiutare le parti interessate a prepararsi ad applicare il regolamento e una campagna di informazione in tutti gli Stati membri, con il sostegno degli uffici di rappresentanza.

1. IL NUOVO QUADRO GIURIDICO DELL'UE IN MATERIA DI PROTEZIONE DEI DATI — MAGGIORE PROTEZIONE E NUOVE OPPORTUNITÀ

Il regolamento continua a seguire l'impostazione della direttiva sulla protezione dei dati ma, basandosi su vent'anni di legislazione dell'UE in materia e di giurisprudenza pertinente, chiarisce e modernizza le norme concernenti tale protezione e introduce alcuni elementi innovativi che rafforzano la tutela dei diritti delle persone e offrono nuove opportunità per le imprese e le attività commerciali, in particolare:

- **un quadro giuridico armonizzato che porta a un'applicazione uniforme delle norme a vantaggio del mercato unico digitale dell'Unione**. Ciò significa un unico insieme di norme per i cittadini e le imprese, che rimedierà alla situazione attuale in cui gli Stati membri dell'Unione applicano le norme della direttiva in modi diversi. Per garantire un'applicazione uniforme e coerente in tutti gli Stati membri è stato introdotto un meccanismo di sportello unico;

- **parità di condizioni per tutte le imprese che operano sul mercato dell'Unione**. Il regolamento impone alle imprese con sede al di fuori dell'UE di applicare le stesse norme vigenti per le imprese stabilite nell'UE quando trattano dati personali in relazione all'offerta di beni e servizi o al monitoraggio del comportamento dei cittadini nell'Unione. Le imprese che operano dall'esterno dell'UE e sono attive sul mercato unico devono, in determinate circostanze, nominare un rappresentante nell'UE al quale i cittadini e le autorità possano rivolgersi in aggiunta o in sostituzione dell'impresa con sede all'estero;

[6] https://ec.europa.eu/commission/sites/beta-political/files/letter-of-intent-2017_it.pdf.

- **i principi di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita**, che creano incentivi ad adottare sin dall'inizio soluzioni innovative in risposta ai problemi di protezione dei dati;

- **diritti dei singoli rafforzati**. Il regolamento introduce nuovi requisiti in materia di trasparenza e diritti rafforzati in materia di informazione, accesso e cancellazione ("diritto all'oblio"); il silenzio o l'inattività non saranno più considerati valide espressioni di consenso, in quanto è richiesto un atto positivo inequivocabile per esprimerlo; è garantita la protezione dei minori online;

- **maggiore controllo dei singoli sui propri dati personali.** Il regolamento stabilisce un **nuovo diritto alla portabilità dei dati**, che permette ai cittadini di chiedere a un'impresa o un'organizzazione la restituzione dei dati personali ad essa forniti sulla base del consenso o di un contratto; consente inoltre la trasmissione diretta di tali dati personali a un'altra impresa od organizzazione, se tecnicamente fattibile. Poiché permette la trasmissione diretta di dati personali da un'impresa od organizzazione a un'altra, tale diritto sosterrà anche la libera circolazione dei dati personali nell'UE, eviterà il "sequestro" di dati personali e incoraggerà la concorrenza tra imprese. Rendendo più facile peri cittadini passare da un fornitore di servizi all'altro si incoraggerà lo sviluppo di nuovi servizi nel contesto della strategia per il mercato unico digitale;

- **maggiore protezione contro la violazione dei dati**. Il regolamento stabilisce un insieme completo di norme sulle violazioni dei dati personali. Fornisce una chiara definizione di "violazione dei dati personali" e introduce un obbligo di notifica all'autorità di controllo entro 72 ore quando la violazione dei dati è suscettibile di presentare un rischio per i diritti e le libertà delle persone fisiche. In alcune circostanze, impone l'obbligo di informare l'interessato della violazione dei dati che lo riguardano. Queste disposizioni assicurano una protezione fortemente rafforzata rispetto alla situazione attuale nell'UE, in cui soltanto i fornitori di servizi di comunicazione elettronica, gli operatori di servizi essenziali e i fornitori di servizi digitali sono tenuti a comunicare le violazioni dei dati a norma, rispettivamente, della direttiva relativa alla vita privata e alle comunicazioni elettroniche[7] e della direttiva sulla sicurezza delle reti e dell'informazione[8];

- **il regolamento conferisce a tutte le autorità di protezione dei dati il potere di infliggere sanzioni pecuniarie ai titolari del trattamento e ai responsabili del**

---

[7] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37). Ai sensi dell'articolo 95 del regolamento generale sulla protezione dei dati, detto regolamento non impone obblighi supplementari alle persone fisiche o giuridiche per quanto riguarda le materie per le quali sono soggette a obblighi specifici aventi lo stesso obiettivo fissati dalla direttiva 2002/58/CE. Ciò significa, ad esempio, che le entità rientranti nel campo di applicazione di detta direttiva sono soggette all'obbligo ivi previsto di notificare le violazioni di dati personali nella misura in cui la violazione riguarda un servizio che rientra nel campo di applicazione materiale della direttiva. Il regolamento generale sulla protezione dei dati non impone loro obblighi aggiuntivi al riguardo.

[8] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016, pag. 1). I soggetti che rientrano nell'ambito di applicazione della direttiva sulla sicurezza delle reti e dell'informazione sono tenuti a notificare gli incidenti aventi un impatto rilevante o sostanziale su alcuni servizi da loro prestati. La notifica degli incidenti a norma di detta direttiva lascia impregiudicato l'obbligo di notifica della violazione previsto dal regolamento.

trattamento. Attualmente non tutte le autorità godono di tale potere. La modifica favorirà una migliore applicazione delle norme. L'ammontare della sanzione pecuniaria può raggiungere 20 milioni di EUR o, nel caso di un'impresa, il 4% del fatturato mondiale annuo;

- **maggiore flessibilità per i titolari del trattamento e i responsabili del trattamento che trattano dati personali, grazie a disposizioni univoche in materia di responsabilità (principio di responsabilizzazione)**. Il regolamento si discosta da un sistema di notifica in favore del principio di responsabilizzazione, attuato tramite obblighi modulabili in funzione del rischio (per esempio l'obbligo di designare un responsabile della protezione dei dati o l'obbligo di svolgere una valutazione d'impatto sulla protezione dei dati). Al fine di agevolare la valutazione del rischio prima di procedere al trattamento, è stato introdotto un nuovo strumento: la valutazione d'impatto sulla protezione dei dati. Quest'ultima è richiesta ogniqualvolta il trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche. A questo proposito, il regolamento indica espressamente tre situazioni: quando un'impresa valuta in modo sistematico e globale gli aspetti personali relativi a una persona (compresa la profilazione), quando un'impresa tratta dati sensibili su larga scala e quando un'impresa si occupa della sorveglianza sistematica su larga scala di una zona accessibile al pubblico. Le autorità nazionali di protezione dei dati devono rendere pubblico l'elenco dei casi per i quali è richiesta la valutazione d'impatto sulla protezione dei dati[9];

- **maggiore chiarezza riguardo agli obblighi dei responsabili del trattamento e alla responsabilità dei titolari del trattamento quando selezionano un responsabile del trattamento**;

- **un sistema di governance moderno per garantire un'applicazione più coerente ed efficace delle norme.** Il sistema prevede poteri armonizzati per le autorità di protezione dei dati, anche per quanto riguarda le sanzioni pecuniarie, e nuovi meccanismi di cooperazione in rete tra tali autorità;

- **la protezione dei dati personali garantita dal regolamento segue i dati al di fuori dell'UE assicurando un livello elevato di protezione**[10]. L'architettura delle norme sui trasferimenti internazionali del regolamento resta sostanzialmente identica a quella della direttiva del 1995, ma la riforma ne chiarisce e semplifica l'impiego e introduce nuovi strumenti per i trasferimenti. Per quanto riguarda le decisioni di adeguatezza, il regolamento introduce un catalogo preciso e dettagliato di elementi dei quali la Commissione deve tenere conto quando valuta se un sistema estero assicuri una protezione adeguata dei dati personali. Il regolamento inoltre formalizza e amplia il numero di strumenti di trasferimento alternativi, come le clausole contrattuali tipo e le norme vincolanti d'impresa.

Il nuovo regolamento per le istituzioni, gli organi, gli uffici e le agenzie dell'Unione[11] e il regolamento sulla vita privata e le comunicazioni elettroniche[12], attualmente in corso di

---

9 Articolo 35 del regolamento.

10 Comunicazione della Commissione "Scambio e protezione dei dati personali in un mondo globalizzato", COM(2017) 7 final.

11 Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi, degli uffici e delle

negoziazione, una volta adottati assicureranno che l'UE disponga di un insieme di norme complete ed efficaci in materia di protezione dei dati[13].

2. ATTIVITÀ PREPARATORIE SVOLTE FINORA A LIVELLO DI UNIONE EUROPEA

Per una fruttuosa applicazione del regolamento è necessaria la cooperazione tra tutti i soggetti interessati alla protezione dei dati: gli Stati membri, le pubbliche amministrazioni, le autorità nazionali di protezione dei dati, le imprese, le organizzazioni che trattano dati personali, i cittadini e la Commissione.

2.1 Azioni della Commissione europea

Poco dopo l'entrata in vigore del regolamento a metà del 2016, la Commissione si è impegnata con le autorità degli Stati membri, le autorità di protezione dei dati e le parti interessate a preparare l'applicazione del regolamento e offrire sostegno e consulenza.

a) Sostegno agli Stati membri e alle autorità nazionali

La Commissione opera in stretta collaborazione con gli Stati membri per sostenerne le attività durante il periodo transitorio e garantire il massimo livello di coerenza possibile. A tal fine ha istituito un gruppo di esperti incaricato di assistere gli Stati membri nei preparativi per l'applicazione del regolamento. Il gruppo, che si è già riunito tredici volte, funge da luogo di scambio di esperienze e competenze tra gli Stati membri[14]. La Commissione ha anche organizzato riunioni bilaterali con le autorità degli Stati membri per discutere le questioni emerse a livello nazionale.

b) Sostegno alle singole autorità di protezione dei dati e all'istituzione del comitato europeo per la protezione dei dati

La Commissione sostiene attivamente le attività del gruppo di lavoro articolo 29, anche al fine di assicurare un'agevole transizione verso il comitato europeo per la protezione dei dati[15].

c) Azione a livello internazionale

Il regolamento rafforzerà ulteriormente la capacità dell'Unione di promuovere in modo attivo i suoi valori in materia di protezione dei dati e faciliterà la circolazione transfrontaliera di

---

agenzie dell'Unione, nonché la libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE, COM(2017) 8 final.

12 Proposta di regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), COM(2017) 10 final.

13 In attesa dell'adozione e dell'entrata in vigore del regolamento sulla vita privata e le comunicazioni elettroniche, la direttiva 2002/58/CE si applica come *lex specialis* rispetto al regolamento.

14 Per un elenco completo delle riunioni, i programmi, le sintesi delle discussioni e il riepilogo dello stato di avanzamento della legislazione nei diversi Stati membri, consultare http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3461&Lang=IT.

15 Per esempio, la Commissione offrirà al comitato europeo per la protezione dei dati la possibilità di usare il sistema di informazione del mercato interno (IMI) per le comunicazioni tra i suoi membri.

questi ultimi incoraggiando la convergenza degli ordinamenti giuridici a livello globale[16]. In ambito internazionale si riconosce sempre più che le norme dell'UE stabiliscono standard di protezione dei dati tra i più elevati del mondo. Anche la convenzione n. 108 del Consiglio d'Europa, l'unico strumento multilaterale giuridicamente vincolante nel settore della protezione dei dati personali, è in fase di modernizzazione. La Commissione si sta adoperando affinché rifletta gli stessi principi sanciti dalle nuove norme dell'UE di protezione dei dati e contribuisca così all'adozione di un insieme uniforme di standard elevati di protezione. La Commissione promuoverà attivamente la rapida adozione del testo modernizzato della convenzione affinché l'UE ne diventi firmataria[17]. La Commissione incoraggia i paesi terzi a ratificare la convenzione n. 108 del Consiglio d'Europa e il relativo protocollo addizionale.

Inoltre, vari paesi e organizzazioni regionali al di fuori dell'UE, dal nostro vicinato immediato all'Asia, l'America latina e l'Africa, stanno adottando una nuova legislazione in materia di protezione dei dati o aggiornando quella esistente, al fine di cogliere le opportunità offerte dall'economia digitale globale e rispondere alla crescente domanda di maggiore sicurezza dei dati e tutela della vita privata. Nonostante le differenze presenti tra i vari paesi in termini di impostazione e livello di sviluppo legislativo, vi sono segni che il regolamento serve sempre più da punto di riferimento e fonte di ispirazione[18].

In questo contesto, la Commissione porta avanti l'azione a livello internazionale in linea con la comunicazione di gennaio 2017[19], impegnandosi attivamente con i principali partner commerciali, segnatamente in Asia orientale e sudorientale e in America latina, in vista della possibile adozione di decisioni di adeguatezza[20].

In particolare, la Commissione collabora con il Giappone per giungere a un accertamento simultaneo di un livello adeguato di protezione da entrambe le parti entro i primi mesi del 2018, come annunciato dal presidente Juncker e dal primo ministro Abe nella dichiarazione congiunta del 6 luglio 2017[21]. Sono stati avviati colloqui anche con la Corea del Sud in vista di una possibile decisione di adeguatezza. L'adozione di una decisione di adeguatezza consentirebbe la libera circolazione dei dati con i paesi terzi interessati garantendo l'applicazione di un elevato livello di protezione allorché i dati personali vengono trasferiti dall'UE verso tali paesi.

Parallelamente, la Commissione collabora con le parti interessate al fine di sfruttare appieno il potenziale dell'insieme di strumenti per i trasferimenti internazionali contenuto nel regolamento generale sulla protezione dei dati, sviluppando meccanismi alternativi di trasferimento dei dati adeguati alle peculiari esigenze di specifici settori e/o operatori[22].

---

16 Documento di riflessione sulla gestione della globalizzazione COM(2017) 240.

17 Convenzione del Consiglio d'Europa del 28 gennaio 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STE N. 108) e protocollo addizionale del 2001 alla convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale, concernente le autorità di controllo ed i flussi transfrontalieri (STE N. 181). La convenzione è aperta all'adesione degli Stati non membri del Consiglio d'Europa ed è già stata ratificata da 51 paesi (tra cui Uruguay, Maurizio, Senegal e Tunisia).

18 Cfr., per esempio, le norme in materia di protezione dei dati degli Stati ibero-americani, http://www.redipd.es/documentacion/common/Estandares_eng_Con_logo_RIPD.pdf.

19 COM(2017) 7.

20 COM(2017) 7 ibid. pagg. 10-11.

21 http://europa.eu/rapid/press-release_STATEMENT-17-1917_en.htm.

22 COM(2017) 7 ibid pag. 10-11.

d) Impegno con le parti interessate

La Commissione ha organizzato varie iniziative rivolte alle parti interessate[23]. Un nuovo seminario rivolto ai consumatori è previsto per il primo trimestre del 2018. Si sono svolte anche discussioni settoriali specifiche in ambiti come quello della ricerca e dei servizi finanziari.

La Commissione ha inoltre istituito un gruppo multilaterale sul regolamento, composto da rappresentanti della società civile e delle imprese, studiosi e professionisti. Tale gruppo fornirà consulenza alla Commissione, in particolare sul modo in cui diffondere un adeguato livello di conoscenza del regolamento tra le parti interessate[24].

Infine, tramite il programma quadro di ricerca e innovazione Orizzonte 2020[25], la Commissione europea ha finanziato azioni destinate a sviluppare strumenti a sostegno dell'applicazione efficace delle disposizioni del regolamento relative al consenso e azioni riguardanti metodi di analisi dei dati che tutelino la vita privata, quali il "multi-party computing" e la crittografia omomorfica.

2.2 Azioni del gruppo di lavoro articolo 29 / comitato europeo per la protezione dei dati

Il gruppo di lavoro articolo 29, che riunisce tutte le autorità nazionali di protezione dei dati, compreso il garante europeo della protezione dei dati, svolge un ruolo fondamentale nei preparativi per l'applicazione del regolamento pubblicando linee guida per le imprese e altre parti interessate. Essendo preposte all'applicazione del regolamento e fungendo da punto di contatto diretto per le parti interessate, le autorità nazionali di protezione dei dati si trovano nella posizione migliore per fornire maggiore certezza del diritto riguardo all'interpretazione del regolamento.

Linee guida/documenti di lavoro adottati dal gruppo di lavoro articolo 29 in vista dell'applicazione del regolamento[26]	
Diritto alla portabilità dei dati	Adottati in data 4-5 aprile 2017
Responsabili della protezione dei dati	
Individuazione dell'autorità di controllo capofila	
Valutazione d'impatto sulla protezione dei dati	Adottato in data 3-4 ottobre 2017
Sanzioni amministrative pecuniarie	Adottato in data 3-4 ottobre 2017
Profilazione	Attività in corso
Violazione dei dati	Attività in corso

[23] Due seminari con il settore a luglio 2016 e aprile 2017, due tavole rotonde con le imprese a dicembre 2016 e maggio 2017, un seminario sui dati sanitari a ottobre 2017 e un seminario con i rappresentanti delle PMI a novembre 2017.

[24] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537&Lang=IT.

[25] https://ec.europa.eu/programmes/horizon2020/h2020-sections.

[26] Tutte le linee guida adottate sono disponibili all'indirizzo: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

Consenso	Attività in corso
Trasparenza	Attività in corso
Certificazione e accreditamento	Attività in corso
Criteri di riferimento per l'adeguatezza	Attività in corso
Norme vincolanti d'impresa per i titolari del trattamento	Attività in corso
Norme vincolanti d'impresa per i responsabili del trattamento	Attività in corso

Il gruppo di lavoro articolo 29 si sta adoperando per aggiornare i pareri esistenti, anche riguardo agli strumenti per il trasferimento di dati verso i paesi terzi.

Poiché è essenziale che gli operatori dispongano di un unico insieme coerente di linee guida, gli attuali orientamenti a livello nazionale devono essere abrogati o allineati a quelli adottati sul medesimo argomento dal gruppo di lavoro articolo 29 / comitato europeo per la protezione dei dati.

La Commissione attribuisce grande importanza al fatto che tali linee guida sono sottoposte a consultazione pubblica prima del perfezionamento. È essenziale che i contributi delle parti interessate a questo processo siano il più possibile precisi e concreti, al fine di agevolare l'individuazione delle migliori prassi e sottoporre gli aspetti settoriali all'attenzione del gruppo di lavoro articolo 29. La responsabilità finale delle linee guida spetta comunque al gruppo di lavoro articolo 29 e al futuro comitato europeo per la protezione dei dati, ai quali le autorità di protezione dei dati faranno riferimento ai fini dell'applicazione del regolamento.

Occorre prevedere la possibilità di modificare le linee guida alla luce degli sviluppi e dell'applicazione pratica. A tal fine, è essenziale che le autorità di protezione dei dati promuovano una cultura del dialogo con tutte le parti interessate, incluse le imprese.

È importante ricordare che, qualora emergano dubbi riguardanti l'interpretazione e l'applicazione del regolamento, spetta agli organi giurisdizionali nazionali e dell'Unione fornire l'interpretazione definitiva del regolamento.

3. PROVVEDIMENTI ANCORA DA ADOTTARE PER UNA PREPARAZIONE OTTIMALE

3.1 Gli Stati membri devono completare l'istituzione del quadro giuridico a livello nazionale

Il regolamento è direttamente applicabile in tutti gli Stati membri[27]. Ciò significa che entra in vigore e si applica senza necessità di alcun atto legislativo nazionale: di norma, i cittadini, le imprese, le pubbliche amministrazioni e altre organizzazioni che trattano dati personali possono basarsi direttamente sulle disposizioni del regolamento. Ciononostante, conformemente al regolamento, gli Stati membri devono adottare le misure necessarie per

[27] Articolo 288 del TFUE.

adattare la rispettiva legislazione abrogando e modificando le leggi esistenti, istituire autorità nazionali di protezione dei dati[28], scegliere un organismo di accreditamento[29] e stabilire le norme per conciliare la libertà di espressione con la protezione dei dati[30].

Il regolamento offre altresì agli Stati membri la possibilità di precisare ulteriormente l'applicazione delle norme in materia di protezione dei dati in ambiti specifici, vale a dire: settore pubblico[31], rapporti di lavoro e sicurezza sociale[32], medicina preventiva e medicina del lavoro, sanità pubblica[33], fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o fini statistici[34], numero di identificazione nazionale[35], accesso del pubblico ai documenti ufficiali[36] e obblighi di segretezza[37]. Inoltre, per quanto riguarda il trattamento di dati genetici, dati biometrici o dati relativi alla salute, il regolamento consente agli Stati membri di mantenere o introdurre ulteriori condizioni, comprese limitazioni[38].

Le azioni degli Stati membri in questo contesto sono delimitate da due elementi:

1. l'articolo 8 della Carta dei diritti fondamentali dell'Unione europea ("Carta"), nel senso che qualsiasi legge nazionale volta a precisare le norme del regolamento deve soddisfare le condizioni previste dall'articolo 8 della Carta (e dal regolamento, che si fonda su detto articolo), e
2. l'articolo 16, paragrafo 2, del TFUE, in base al quale la legislazione nazionale non può interferire con la libera circolazione dei dati personali all'interno dell'Unione.

Il regolamento offre l'opportunità di semplificare l'ambiente giuridico riducendo così il numero di norme nazionali e garantendo maggiore chiarezza per gli operatori.

Quando adattano la legislazione nazionale, gli Stati membri devono tenere conto del fatto che qualsiasi misura nazionale suscettibile di ostacolare l'applicabilità diretta del regolamento e comprometterne l'applicazione simultanea e uniforme in tutto il territorio dell'Unione è in contrasto con i trattati[39].

È altresì vietato integrare il testo dei regolamenti nel diritto nazionale (per esempio ripetere le definizioni o i diritti dei singoli), a meno che tale integrazione sia strettamente necessaria ai

---

28 Articolo 54, paragrafo 1, del regolamento.

29 L'articolo 43, paragrafo 1, del regolamento prevede che gli Stati membri offrano agli organismi di certificazione due possibili metodi di accreditamento, ossia: da parte dell'autorità di controllo nazionale della protezione dei dati istituita a norma della legislazione in materia di protezione dei dati e/o da parte dell'organismo di accreditamento nazionale istituito ai sensi del regolamento (CE) n. 765/2008 relativo all'accreditamento e alla vigilanza del mercato. A tal fine, la cooperazione europea per l'accreditamento ("EA", riconosciuta ai sensi del regolamento (CE) n. 765/2008), che riunisce gli organismi nazionali di accreditamento, e le autorità di controllo istituite a norma del regolamento dovrebbero operare in stretta collaborazione.

30 Articolo 85, paragrafo 1, del regolamento.

31 Articolo 6, paragrafo 2, del regolamento.

32 Articolo 88 e articolo 9, paragrafo 2, lettera b), del regolamento. Il pilastro europeo dei diritti sociali stabilisce inoltre che: "*I lavoratori hanno diritto alla protezione dei propri dati personali nell'ambito del rapporto di lavoro*" (2017/C 428/09, GU C 428 del 13.12.2017, pag. 10).

33 Articolo 9, paragrafo 2, lettere h) e i), del regolamento.

34 Articolo 9, paragrafo 2, lettera j), del regolamento.

35 Articolo 87 del regolamento.

36 Articolo 86 del regolamento.

37 Articolo 90 del regolamento.

38 Articolo 9, paragrafo 4, del regolamento.

39 Causa 94/77 *Fratelli Zerbone Snc / Amministrazione delle finanze dello Stato*, ECLI:EU:C:1978:17.

fini della coerenza e per rendere le disposizioni nazionali comprensibili alle persone cui si applicano[40]. La riproduzione del testo del regolamento parola per parola nella legge nazionale di precisazione è ammessa solo in circostanze eccezionali e giustificate e non può essere usata per inserire condizioni o interpretazioni aggiuntive al testo del regolamento.

L'interpretazione del regolamento spetta agli organi giurisdizionali europei (giudici nazionali e, da ultimo, Corte di giustizia dell'Unione europea) e non ai legislatori degli Stati membri. Il legislatore nazionale pertanto non può copiare il testo del regolamento se non è necessario alla luce dei criteri forniti dalla giurisprudenza, né interpretarlo o inserire condizioni aggiuntive alle norme direttamente applicabili in virtù del regolamento. Se lo facesse, gli operatori nell'Unione si troverebbero di nuovo di fronte a un quadro frammentato e non saprebbero quali norme sono tenuti a rispettare.

In questa fase soltanto due Stati membri hanno già adottato la legislazione nazionale pertinente[41]; gli altri Stati membri hanno raggiunto diversi stadi delle rispettive procedure legislative[42] e prevedono di adottare la normativa entro il 25 maggio 2018. È importante concedere agli operatori un periodo sufficiente a prepararsi per tutte le disposizioni alle quali devono conformarsi.

Qualora gli Stati membri non adottino le misure necessarie a norma del regolamento, non le adottino entro i termini previsti o facciano ricorso alle disposizioni del regolamento relative alle precisazioni in modo contrario al regolamento stesso, la Commissione intende avvalersi di tutti gli strumenti di cui dispone, compreso il ricorso alla procedura di infrazione.

3.2 Le autorità di protezione dei dati devono garantire la piena operatività del nuovo e indipendente comitato europeo per la protezione dei dati

È essenziale che il nuovo organismo istituito dal regolamento, il comitato europeo per la protezione dei dati[43], successore del gruppo di lavoro articolo 29, sia pienamente operativo a partire dal 25 maggio 2018.

Il garante europeo della protezione dei dati, ossia l'autorità di protezione dei dati responsabile di vigilare sulle istituzioni e gli organismi dell'Unione, metterà a disposizione del comitato europeo per la protezione dei dati un segretariato, al fine di migliorare le sinergie e l'efficacia. Nei mesi scorsi ha avviato i preparativi necessari a tal fine.

Il comitato europeo per la protezione dei dati sarà al centro della protezione dei dati in Europa. Contribuirà all'applicazione coerente della legislazione in materia di protezione dei dati e fornirà una solida base per la cooperazione tra le autorità competenti, compreso il

---

40 Considerando 8 del regolamento.

41 Austria (http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.pdf); Germania (https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1513091793362).

42 Per una panoramica dello stato di avanzamento del processo legislativo nei diversi Stati membri, consultare: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3461&Lang=IT.

43 Il comitato europeo per la protezione dei dati sarà un organismo dell'Unione dotato di personalità giuridica incaricato di garantire l'applicazione coerente del regolamento. Sarà composto dalla figura di vertice di ciascuna autorità di protezione dei dati e dal garante europeo della protezione dei dati, o dai rispettivi rappresentanti.

garante europeo della protezione dei dati. Il comitato europeo per la protezione dei dati non si limiterà a pubblicare linee guida sul modo in cui interpretare i concetti fondamentali del regolamento, ma sarà anche chiamato ad adottare decisioni vincolanti sulle controversie riguardanti il trattamento dei dati a livello transfrontaliero. Ciò garantirà l'applicazione uniforme delle norme dell'Unione e impedirà che la stessa situazione sia gestita in modo diverso nei vari Stati membri.

Il funzionamento regolare ed efficiente del comitato europeo per la protezione dei dati è dunque una condizione essenziale per il buon funzionamento del sistema nel suo insieme. Ora più che mai il comitato dovrà creare una cultura di protezione dei dati comune fra tutte le autorità nazionali di protezione dei dati allo scopo di garantire l'interpretazione coerente delle disposizioni del regolamento. Il regolamento promuove la cooperazione tra le autorità di protezione dei dati dotandole di strumenti per cooperare in modo efficace ed efficiente: in particolare, potranno effettuare operazioni congiunte, adottare decisioni concordate e risolvere eventuali divergenze riguardanti l'interpretazione del regolamento in seno al comitato mediante pareri e decisioni vincolanti. La Commissione incoraggia le autorità di protezione dei dati ad accogliere questi cambiamenti e ad adeguare le rispettive modalità di lavoro, funzionamento e finanziamento per potersi conformare ai nuovi diritti e obblighi.

3.3 Gli Stati membri devono mettere a disposizione delle autorità nazionali di protezione dei dati le necessarie risorse umane e finanziarie

L'istituzione di autorità di controllo pienamente indipendenti in ciascuno Stato membro è essenziale per garantire la tutela delle persone fisiche con riguardo al trattamento dei loro dati personali nell'Unione[44]. Le autorità di controllo possono proteggere in modo efficace i diritti e le libertà delle persone soltanto se operano in totale indipendenza. Qualsiasi tentativo di minare la loro indipendenza e l'esercizio effettivo dei loro poteri determina un impatto estremamente negativo sull'applicazione della legislazione in materia di protezione dei dati[45].

Il regolamento codifica la condizione che ogni autorità di protezione dei dati agisce in piena indipendenza[46]. Rafforza l'indipendenza delle autorità nazionali di protezione dei dati e le dota di poteri uniformi in tutta l'Unione, in modo che dispongano degli strumenti adeguati per gestire con efficacia i reclami, svolgere indagini efficaci, adottare decisioni vincolanti e imporre sanzioni efficaci e dissuasive. Conferisce loro anche il potere di infliggere ai titolari del trattamento o ai responsabili del trattamento sanzioni amministrative pecuniarie fino a 20 milioni di EUR o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Le autorità di protezione dei dati sono gli interlocutori naturali e il primo punto di contatto per i cittadini, le imprese e le pubbliche amministrazioni per le questioni riguardanti il regolamento. Fra i loro compiti rientra quello di informare i titolari del trattamento e i responsabili del trattamento dei loro obblighi e di promuovere la conoscenza e migliorare la comprensione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento. Ciò non significa tuttavia che i titolari del trattamento e i responsabili del trattamento possano aspettarsi di ricevere dalle autorità di protezione dei dati il tipo di

---

[44] Considerando 117 e già affermato in precedenza nel considerando 62 della direttiva 95/46.

[45] Comunicazione della Commissione al Parlamento europeo e al Consiglio sul seguito dato al programma di lavoro per una migliore applicazione della direttiva sulla protezione dei dati, COM(2007) 87 def., 7 marzo 2007.

[46] Articolo 52 del regolamento.

consulenza giuridica personalizzata e su misura che solo un legale o un responsabile della protezione dei dati è in grado di fornire.

Le autorità nazionali di protezione dei dati svolgono quindi un ruolo centrale, ma il relativo squilibrio tra le risorse umane e finanziarie loro assegnate nei diversi Stati membri può comprometterne l'efficacia e, in definitiva, la piena indipendenza prescritta dal regolamento. Può anche avere ripercussioni negative sul modo in cui le autorità di protezione dei dati possono esercitare i loro poteri, per esempio quelli di indagine. Gli Stati membri sono incoraggiati a ottemperare all'obbligo giuridico di dotare la rispettiva autorità nazionale di protezione dei dati delle risorse umane, tecniche e finanziarie, dei locali e delle infrastrutture necessari per l'effettivo adempimento dei suoi compiti e l'esercizio dei propri poteri[47].

3.4 Le imprese, le pubbliche amministrazioni e le altre organizzazioni che trattano dati devono prepararsi ad applicare le nuove norme

Il regolamento non ha modificato in modo sostanziale i concetti e i principi fondamentali della legislazione in materia di protezione dei dati introdotta nel 1995. La grande maggioranza dei titolari del trattamento e dei responsabili del trattamento che rispettano già le attuali disposizioni dell'UE non dovrà quindi introdurre importanti modifiche nelle proprie operazioni di trattamento dei dati per conformarsi al regolamento.

Il regolamento produce effetti per la maggior parte degli operatori le cui attività principali consistono nel trattamento dei dati e/o nel trattamento di dati sensibili, nonché per gli operatori che si occupano del monitoraggio regolare e sistematico delle persone fisiche su larga scala. Questi operatori, con tutta probabilità, dovranno nominare un responsabile della protezione dei dati, svolgere una valutazione d'impatto sulla protezione dei dati e notificare le violazioni dei dati in presenza di un rischio per i diritti e le libertà delle persone. Per contro, gli operatori, in particolare le PMI, la cui attività principale non consista in trattamenti dei dati che comportano un rischio elevato non saranno di norma soggetti a questi obblighi specifici previsti dal regolamento.

È importante che i titolari del trattamento e i responsabili del trattamento svolgano riesami completi della loro politica in materia di dati al fine di individuare chiaramente quali dati conservano, per quali finalità e su quale base giuridica (per esempio ambiente cloud; operatori del settore finanziario). Devono inoltre esaminare i contratti in vigore, in particolare quelli tra titolari del trattamento e responsabili del trattamento, le modalità di trasferimento internazionale e la governance generale (quali misure informatiche e organizzative adottare), compresa la nomina di un responsabile della protezione dei dati. Un elemento essenziale di questo processo è garantire che i più alti livelli dirigenziali partecipino a tali riesami, forniscano il loro contributo e siano periodicamente aggiornati e consultati in merito alle modifiche della politica aziendale in materia di dati.

A tal fine, alcuni operatori fanno ricorso a liste di controllo della conformità (interne o esterne), si rivolgono a società di consulenza e studi legali e cercano prodotti in grado di soddisfare i requisiti di protezione dei dati fin dalla progettazione e per impostazione predefinita. Ogni settore deve mettere a punto meccanismi idonei alla natura specifica del proprio ambito di attività e adatti al rispettivo modello commerciale.

---

[47] Articolo 52, paragrafo 4, del regolamento.

Le imprese e le altre organizzazioni che trattano dati potranno inoltre avvalersi dei nuovi strumenti previsti dal regolamento come elemento per dimostrare la conformità, per esempio i codici di condotta e i meccanismi di certificazione. Si tratta di approcci dal basso verso l'alto mutuati dalla comunità imprenditoriale, dalle associazioni o altre organizzazioni che rappresentano le categorie di titolari del trattamento e responsabili del trattamento e riflettono le migliori prassi, importanti sviluppi in un determinato settore o possono fornire indicazioni in merito al livello di protezione dei dati richiesto da alcuni prodotti e servizi. Il regolamento prevede un insieme organico di norme per tali meccanismi, tenendo conto delle realtà di mercato (per esempio certificazione da parte di un organismo di certificazione o di un'autorità di protezione dei dati).

Tuttavia le grandi imprese si stanno preparando attivamente ad applicare le nuove norme, mentre molte PMI non hanno ancora acquisito piena consapevolezza delle loro implicazioni.

In breve, gli operatori dovrebbero prepararsi e adeguarsi alle nuove norme e vedere il regolamento come:

- un'opportunità per regolarizzare la propria situazione in termini di dati personali che trattano e modalità di gestione dei dati;
- un obbligo di sviluppare prodotti compatibili con la tutela della vita privata e la protezione dei dati e di instaurare un nuovo rapporto con la clientela basato sulla fiducia e sulla trasparenza;
- un'opportunità per reimpostare le relazioni con le autorità di protezione dei dati attraverso la responsabilizzazione e la conformità proattiva.

3.5 Informare le parti interessate, in particolare i cittadini e le piccole e medie imprese

Il successo del regolamento dipende da un'adeguata sensibilizzazione di tutte le parti interessate alle nuove norme (le imprese e le altre organizzazioni che trattano dati, il settore pubblico e i cittadini). A livello nazionale, il compito di svolgere un'opera di sensibilizzazione e fungere da primo punto di contatto per i titolari del trattamento, i responsabili del trattamento e i cittadini spetta principalmente alle autorità di protezione dei dati. Essendo preposte all'applicazione delle norme in materia di protezione dei dati nel rispettivo territorio, tali autorità sono anche nella migliore posizione per spiegare alle imprese e al settore pubblico i cambiamenti introdotti dal regolamento e far sì che i cittadini conoscano bene i loro diritti.

Le autorità di protezione dei dati hanno cominciato a informare le parti interessate secondo l'impostazione specifica nazionale. Alcune organizzano seminari con le pubbliche amministrazioni, anche a livello regionale e locale, e incontri con i diversi settori di attività al fine di migliorare la conoscenza delle principali disposizioni del regolamento. Altre offrono programmi di formazione specifici per i responsabili della protezione dei dati. Quasi tutte mettono a disposizione materiali informativi in varie forme (liste di controllo, video, ecc.) sul proprio sito Internet.

Ciononostante, i cittadini in generale non conoscono ancora a sufficienza le modifiche e i diritti rafforzati che saranno introdotti dalle nuove norme in materia di protezione dei dati. Le autorità di protezione dei dati dovrebbero proseguire e intensificare le iniziative di formazione e sensibilizzazione intraprese, prestando particolare attenzione alle PMI. Inoltre, le amministrazioni nazionali settoriali possono sostenere le attività delle autorità di protezione dei dati e, sulla base dei contributi di queste ultime, svolgere le proprie attività di sensibilizzazione tra le varie parti interessate.

4. PROSSIME TAPPE

Nei prossimi mesi la Commissione continuerà a sostenere attivamente tutti i soggetti interessati nei preparativi per l'applicazione del regolamento.

a) Collaborazione con gli Stati membri

La Commissione continuerà a collaborare con gli Stati membri nella fase preparatoria fino a maggio 2018. A partire da maggio 2018 controllerà in che modo gli Stati membri applicano le nuove norme adottando opportuni provvedimenti ove necessario.

b) Nuovi orientamenti online in tutte le lingue dell'Unione e attività di sensibilizzazione

La Commissione sta mettendo a disposizione orientamenti pratici[48] per aiutare le imprese, in particolare le PMI, le autorità pubbliche e i cittadini a conformarsi alle nuove norme in materia di protezione dei dati e a trarne beneficio.

Gli orientamenti sono forniti sotto forma di strumento pratico online disponibile in tutte le lingue dell'UE. Tale strumento sarà aggiornato periodicamente ed è rivolto a tre principali destinatari: cittadini, imprese (in particolare le PMI) e altre organizzazioni e pubbliche amministrazioni. Comprende domande e risposte selezionate in base ai riscontri ricevuti dalle parti interessate, con esempi pratici e collegamenti a varie fonti di informazioni (per esempio articoli del regolamento, linee guida del gruppo di lavoro articolo 29 / comitato europeo per la protezione dei dati e materiali elaborati a livello nazionale).

La Commissione aggiornerà periodicamente lo strumento, aggiungendo domande e aggiornando le risposte sulla base dei riscontri ricevuti e alla luce di ogni nuovo aspetto che possa emergere durante l'applicazione.

Gli orientamenti saranno promossi tramite una campagna di informazione e attività di divulgazione rivolte alle imprese e ai cittadini in tutti gli Stati membri.

Poiché il regolamento prevede diritti dei singoli rafforzati, la Commissione avvierà altresì attività di sensibilizzazione e parteciperà ad eventi nei vari Stati membri allo scopo di informare i cittadini sui vantaggi e sull'impatto del regolamento.

c) Sostegno finanziario alle campagne di informazione e sensibilizzazione a livello nazionale

La Commissione sostiene le iniziative di sensibilizzazione e gli sforzi di adempimento intrapresi a livello nazionale concedendo sovvenzioni che possono essere usate per organizzare attività di formazione presso le autorità di protezione dei dati, le pubbliche amministrazioni, i professionisti legali e i responsabili della protezione dei dati[49] e permettere loro di prendere dimestichezza con il regolamento.

---

[48] Gli orientamenti contribuiranno a una migliore comprensione delle norme dell'UE in materia di protezione dei dati, ma soltanto il testo del regolamento ha efficacia giuridica. Di conseguenza, solo il regolamento può creare diritti e obblighi per i singoli.

[49] Sovvenzioni concesse nell'ambito del programma "Diritti e cittadinanza" 2016 https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/rec/calls/rec-data-2016.html#c,topics=callIdentifier/t/REC-DATA-2016/1/1/1/default-

Circa 1,7 milioni di EUR saranno assegnati a sei beneficiari che coprono più della metà degli Stati membri dell'Unione. I finanziamenti saranno destinati alle autorità pubbliche locali, compresi i responsabili della protezione dei dati delle autorità pubbliche locali, delle autorità pubbliche e del settore privato, nonché a giudici e professionisti legali. Le sovvenzioni saranno impiegate per elaborare materiale didattico per le autorità di protezione dei dati, i responsabili della protezione dei dati e altri professionisti, nonché per programmi di formazione dei formatori.

La Commissione ha anche pubblicato un invito a presentare proposte specificamente rivolto alle autorità di protezione dei dati. Sarà disponibile una dotazione complessiva di 2 milioni di EUR per sostenere le attività di sensibilizzazione rivolte alle parti interessate[50]. L'obiettivo è fornire un cofinanziamento dell'80% per le misure adottate dalle autorità di protezione dei dati nel periodo 2018-2019 per sensibilizzare le imprese, in particolare le PMI, e rispondere alle loro richieste di informazioni. Il finanziamento può essere usato anche per attività di sensibilizzazione rivolte ai cittadini.

d) Valutazione della necessità di fare ricorso ai poteri conferiti alla Commissione

Il regolamento[51] conferisce alla Commissione il potere di adottare atti di esecuzione o atti delegati per sostenere ulteriormente l'applicazione delle nuove norme. La Commissione intende avvalersi di tale potere solo in presenza di un valore aggiunto chiaramente dimostrato e sulla base dei riscontri ricevuti nell'ambito della consultazione delle parti interessate. In particolare, la Commissione esaminerà la questione della certificazione sulla base di uno studio condotto da esperti esterni e dei contributi e pareri al riguardo forniti dal gruppo multilaterale sul regolamento istituito alla fine del 2017. In questo contesto sarà pertinente anche l'attività svolta dall'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) nel settore della cibersicurezza.

e) Integrazione del regolamento nell'accordo SEE

La Commissione porterà avanti l'attività con i tre Stati EFTA (Islanda, Liechtenstein e Norvegia) nello Spazio economico europeo (SEE) volta a integrare il regolamento nell'accordo SEE[52]. I dati personali potranno circolare liberamente tra l'UE e i paesi del SEE come avviene tra gli Stati membri dell'Unione soltanto dopo l'entrata in vigore dell'integrazione del regolamento nell'accordo SEE.

---

group&callStatus/t/Forthcoming/1/1/0/default-group&callStatus/t/Open/1/1/0/default-group&callStatus/t/Closed/1/1/0/default-group&+identifier/desc).

50 http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/rec/topics/rec-rdat-trai-ag-2017.html.

51 Atto delegato per stabilire le informazioni da presentare sotto forma di icona e le procedure per fornire icone standardizzate (articolo 12, paragrafo 8, del regolamento); atto delegato per precisare i requisiti di cui tenere conto per i meccanismi di certificazione (articolo 43, paragrafo 8, del regolamento); atto di esecuzione per stabilire norme tecniche riguardanti i meccanismi di certificazione e i sigilli e marchi di protezione dei dati e le modalità per promuovere e riconoscere tali meccanismi di certificazione, i sigilli e marchi di protezione dei dati (articolo 43, paragrafo 9, del regolamento); atto di esecuzione per specificare il formato e le procedure per lo scambio di informazioni tra titolari del trattamento, responsabili del trattamento e autorità di controllo in merito alle norme vincolanti d'impresa (articolo 47, paragrafo 3, del regolamento); atto di esecuzione per specificare il formato e le procedure per l'assistenza reciproca e le modalità per lo scambio di informazioni per via elettronica tra autorità di controllo (articolo 61, paragrafo 9, e articolo 67 del regolamento).

52 Per informazioni sullo stato di avanzamento, consultare: http://www.efta.int/eea-lex/32016R0679.

f) Recesso del Regno Unito dall'Unione europea

Nel contesto dei negoziati tra l'Unione europea e il Regno Unito per la conclusione di un accordo di recesso a norma dell'articolo 50 del trattato sull'Unione europea, la Commissione perseguirà l'obiettivo di assicurare che le disposizioni del diritto dell'Unione in materia di protezione dei dati personali applicabili il giorno precedente la data del recesso continuino ad applicarsi ai dati personali trattati nel Regno Unito prima della data del recesso[53]. Per esempio, i singoli interessati dovranno continuare ad avere il diritto di essere informati, il diritto di accesso, il diritto di rettifica, il diritto alla cancellazione, il diritto di limitazione del trattamento, il diritto alla portabilità dei dati e il diritto di opporsi al trattamento e di non essere sottoposti a una decisione basata unicamente sul trattamento automatizzato, sulla base delle pertinenti disposizioni del diritto dell'Unione applicabili alla data del recesso. I dati personali di cui sopra dovranno essere conservati per un periodo non superiore al conseguimento delle finalità per le quali sono stati trattati.

A decorrere dalla data del recesso, e fatte salve eventuali disposizioni transitorie contenute nell'accordo di recesso, al Regno Unito si applicheranno le norme del regolamento relative ai trasferimenti di dati personali verso paesi terzi[54].

g) Punto della situazione a maggio 2019

Dopo il 25 maggio 2018 la Commissione seguirà da vicino l'applicazione delle nuove norme e sarà pronta ad adottare provvedimenti qualora emergano problemi rilevanti. Un anno dopo l'inizio dell'applicazione del regolamento (2019) la Commissione organizzerà un'iniziativa per fare il bilancio delle esperienze maturate dalle diverse parti interessate nell'applicazione del regolamento. I risultati dell'iniziativa saranno anche integrati nella relazione di valutazione e sul riesame del regolamento che la Commissione è tenuta a presentare entro maggio 2020. La relazione esaminerà, in particolare, i trasferimenti internazionali e le disposizioni in materia di cooperazione e coerenza attinenti all'attività delle autorità di protezione dei dati.

Conclusioni

Il 25 maggio un nuovo, unico insieme di norme in materia di protezione dei dati entrerà pienamente in vigore in tutta l'Unione. Il nuovo quadro giuridico apporterà notevoli benefici per i cittadini, le imprese, le pubbliche amministrazioni e altre organizzazioni. Esso, inoltre, offre all'Unione l'opportunità di diventare un leader globale nel campo della protezione dei dati personali. Tuttavia, la riforma può avere successo soltanto se tutti gli interessati rispettano i propri obblighi e godono dei propri diritti.

Sin dall'adozione del regolamento nel maggio 2016, la Commissione si è impegnata attivamente con tutti i soggetti interessati – governi, autorità nazionali, imprese, società civile – in vista dell'applicazione delle nuove norme. Buona parte dell'attività è stata dedicata a garantire un'ampia conoscenza delle norme e la piena preparazione ad applicarle, ma resta ancora altro lavoro da svolgere. I preparativi procedono a varie velocità nei diversi Stati

---

[53] https://ec.europa.eu/commission/publications/position-paper-use-data-and-protection-information-obtained-or-processed-withdrawal-date_en.

[54] Cfr. comunicazione della Commissione alle parti interessate "*Withdrawal of the United Kingdom from the Union and EU rules in the field of data protection*" (Recesso del Regno Unito dall'Unione e norme dell'UE nel settore della protezione dei dati, http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=49245).

membri e presso i vari soggetti interessati. Inoltre, la conoscenza dei vantaggi e delle opportunità offerti dalle nuove norme non è omogenea. Sussiste, in particolare, la necessità di rafforzare le attività di sensibilizzazione e sostenere gli sforzi di adempimento delle PMI.

La Commissione invita pertanto tutti i soggetti interessati a intensificare le attività in corso per garantire l'applicazione e l'interpretazione coerente delle nuove norme in tutta l'Unione e diffonderne la conoscenza tra le imprese e i cittadini. La Commissione sosterrà tali sforzi con finanziamenti e assistenza amministrativa e contribuirà alle iniziative di sensibilizzazione, in particolare varando lo strumentario di orientamento online.

I dati stanno diventando estremamente preziosi per l'economia odierna e sono elementi essenziali nella vita quotidiana dei cittadini. Le nuove norme offrono un'opportunità unica tanto alle imprese quanto ai cittadini. Le imprese, soprattutto quelle di piccole dimensioni, potranno beneficiare di un unico insieme di norme favorevoli all'innovazione e regolarizzare la propria situazione in termini di dati personali per recuperare la fiducia dei consumatori e sfruttarlo come vantaggio competitivo in tutta l'Unione. I cittadini potranno beneficiare della maggiore protezione dei dati personali ed esercitare un maggiore controllo sulle modalità di gestione dei dati da parte delle imprese.

In un mondo moderno con un'economia digitale in piena espansione l'Unione europea, i suoi cittadini e le sue imprese devono essere pienamente in grado di cogliere i benefici e comprendere le conseguenze dell'economia dei dati. Il nuovo regolamento offre gli strumenti necessari per rendere l'Europa idonea al XXI secolo.

La Commissione intende intraprendere le azioni seguenti.

Nei riguardi degli Stati membri

- La Commissione continuerà a collaborare con gli Stati membri per promuovere la coerenza e limitare la frammentazione nell'applicazione del regolamento, tenendo conto del margine di precisazione di cui godono gli Stati membri ai sensi della nuova legislazione.

- Dopo maggio 2018 la Commissione seguirà da vicino l'applicazione del regolamento negli Stati membri e adotterà opportuni provvedimenti ove necessario, compreso il ricorso alla procedura di infrazione.

Nei riguardi delle autorità di protezione dei dati

- Fino a maggio 2018 la Commissione sosterrà il lavoro delle autorità di protezione dei dati nel contesto del gruppo di lavoro articolo 29 e nella transizione verso il futuro comitato europeo per la protezione dei dati; dopo maggio 2018 contribuirà alle attività del comitato.

- Nel periodo 2018-2019 la Commissione cofinanzierà (dotazione complessiva fino a 2 milioni di EUR) le attività di sensibilizzazione svolte dalle autorità di protezione dei dati a livello nazionale (progetti attuati a partire dalla metà del 2018).

Nei riguardi delle parti interessate

- La Commissione attiverà uno strumento di orientamento pratico online, comprendente domande e risposte, rivolto ai cittadini, alle imprese e alle pubbliche amministrazioni. La Commissione intende promuovere tale strumento fra i destinatari tramite una campagna di informazione rivolta alle imprese e ai cittadini nell'imminenza di maggio 2018 e nel periodo successivo.

- Nel 2018 e anche in seguito la Commissione continuerà a impegnarsi attivamente con le parti interessate, in particolare tramite il gruppo multilaterale sull'attuazione del regolamento e sul livello di conoscenza delle nuove norme;

Nei riguardi di tutti i soggetti interessati

- Nel periodo 2018-2019 la Commissione valuterà la necessità di fare ricorso al suo potere di adottare atti delegati o atti di esecuzione.

- Nel maggio 2019 la Commissione farà un bilancio dell'applicazione del regolamento e nel 2020 presenterà una relazione sull'applicazione delle nuove norme.