Parere congiunto EDPB-GEPD 3/2022 sulla proposta di regolamento sullo spazio europeo dei dati sanitari

Adottato il 12 luglio 2022

INDICE

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Sintesi

Tramite il presente parere congiunto, il comitato europeo per la protezione dei dati (EDPB) e il Garante europeo della protezione dei dati (GEPD) intendono richiamare l'attenzione su alcune problematiche generali in merito alla proposta sullo spazio europeo dei dati sanitari ed a esortare i colegislatori ad adottare misure decisive.

EDPB e GEPD rilevano che la proposta mira a sostenere le persone ad assumere il controllo dei propri dati sanitari, sostenere l'uso di tali dati per una migliore prestazione di assistenza sanitaria, per una ricerca, un'innovazione e una definizione delle politiche migliori, nonché per consentire all'UE di fare pieno uso del potenziale offerto da uno scambio, un uso e un riutilizzo sicuri e protetti di dati sanitari. In effetti, "agevolare l'uso dei dati sanitari elettronici", ai fini tanto dell'uso primario quanto di quello secondario di tali dati, potrebbe contribuire in modo significativo sia agli interessi pubblici sia all'interesse dei singoli interessati/pazienti.

Sebbene lo sforzo per rafforzare il controllo e i diritti degli interessati in merito ai loro dati sanitari personali sia accolto favorevolmente, occorre evidenziare che la proposta in esame prevede principalmente alcune "aggiunte" ad alcuni dei diritti degli interessati già previsti dal regolamento generale sulla protezione dei dati (GDPR). Di fatto la proposta potrebbe persino indebolire la protezione dei diritti alla tutela della vita privata e alla protezione dei dati, in particolare in considerazione delle categorie di dati personali e delle finalità connesse all'uso secondario dei dati.

EDPB e GEPD rilevano che le disposizioni della proposta in questione aggiungeranno un ulteriore livello alla già complessa (caratterizzata da più livelli) raccolta di disposizioni (presenti tanto nel diritto dell'Unione quanto nel diritto degli Stati membri) in materia di trattamento dei dati sanitari (nel settore sanitario). L'interazione tra tali diversi atti legislativi deve essere cristallina.

In particolare EDPB e GEPD ritengono importante chiarire il rapporto tra le disposizioni della proposta in esame e quelle contenute nel GDPR e nelle leggi degli Stati membri. EDPB e GEPD riconoscono l'intenzione e gli sforzi compiuti, nella proposta sullo spazio europeo dei dati sanitari in esame, per rimanere all'interno dei confini tracciati dal GDPR. Ciò può essere rilevato ad esempio quando la proposta crea, mediante il diritto dell'Unione, basi giuridiche e/o eccezioni per il trattamento dei dati sanitari che si inseriscono nella struttura prevista agli articoli 6 e 9 del GDPR. Tuttavia, per quanto concerne il livello di chiarezza auspicato in relazione a tali disposizioni, sono necessari ancora notevoli sforzi (in termini di miglioramento delle disposizioni e di ulteriori chiarimenti), in particolare per quanto concerne l'interazione delle disposizioni con le leggi degli Stati membri ai sensi dell'articolo 9, paragrafo 4, GDPR. Tali preoccupazioni si rispecchiano nelle osservazioni riguardanti i capitoli II e IV della proposta.

Per quanto concerne l'ambito di applicazione della proposta, EDPB e GEPD raccomandano di escludere dall'articolo 33, paragrafo 1, lettera f), della proposta rispettivamente le applicazioni per il benessere e altre applicazioni digitali, così come i dati relativi al benessere e ai comportamenti pertinenti per la salute. In caso di conservazione di tali dati, il trattamento per l'uso secondario di dati personali derivanti da applicazioni per il benessere e altre applicazioni digitali dovrebbe essere subordinato al consenso preventivo ai sensi del GDPR. Inoltre EDPB e GEPD ricordano che tale trattamento può rientrare nell'ambito di applicazione della

direttiva 2002/58/CE ("direttiva relativa alla vita privata e alle comunicazioni elettroniche" o "direttiva e-privacy").

EDPB e GEPD raccomandano inoltre vivamente di non estendere l'ambito di applicazione delle eccezioni al GDPR per quanto concerne i diritti dell'interessato alla proposta e in particolare all'articolo 38, paragrafo 2, della proposta. Tale esenzione pregiudica la possibilità per gli interessati di esercitare un controllo efficace sui loro dati personali piuttosto che rafforzarlo e sembra quindi essere in contrasto con l'obiettivo di cui all'articolo 1, paragrafo 2, lettera a), della proposta.

EDPB e GEPD accolgono con favore il fatto che la proposta faccia riferimento ai diritti di cui al GDPR (ad esempio il diritto di accesso gratuito e il diritto di ottenere una copia dei dati). Tuttavia EDPB e GEPD rilevano che la descrizione dei diritti così come fornita nella proposta non è coerente con quella di cui al GDPR. Come accennato in precedenza, ciò può comportare incertezza del diritto negli interessati che potrebbero non essere in grado di distinguere tra i due tipi di diritti. A tal fine, così come al fine di evitare complessità nell'attuazione pratica, EDPB e GEPD esortano il colegislatore a garantire chiarezza giuridica in merito all'interazione tra i diritti dell'interessato introdotti dalla proposta e le disposizioni generali contenute nel GDPR in merito ai diritti degli interessati.

EDPB e GEPD riconoscono le disposizioni del capo III che mirano a migliorare l'interoperabilità delle cartelle cliniche elettroniche e ad agevolare la connettività di applicazioni mobili per il benessere con tali cartelle cliniche elettroniche. Tuttavia EDPB e GEPD sono del parere che queste ultime non dovrebbero essere incluse nell'uso secondario dei dati sanitari di cui al capo IV della proposta, innanzitutto in considerazione del fatto che i dati sanitari generati dalle applicazioni per il benessere e da applicazioni di sanità digitale non sono soggetti agli stessi requisiti in materia di qualità dei dati e non presentano le stesse caratteristiche di quelli generati da dispositivi medici. Inoltre tali applicazioni generano un'enorme quantità di dati e possono essere altamente invasive in quanto tali dati fanno riferimento a ogni azione che le persone compiono nella loro vita quotidiana. Anche qualora fosse effettivamente possibile separare i dati sanitari da altri tipi di dati, sarebbe comunque semplice trarre deduzioni ad esempio in merito alle pratiche alimentari e altre abitudini, che rivelerebbero informazioni particolarmente sensibili quali l'orientamento religioso.

Per quanto riguarda le finalità dell'uso secondario dei dati sanitari di cui all'articolo 34, paragrafo 1, della proposta, EDPB e GEPD comprendono che l'articolo 34, paragrafo 1, lettere f) e g), della proposta può comprendere qualsiasi forma di "attività di sviluppo e innovazione per prodotti o servizi che contribuiscono alla sanità pubblica o alla sicurezza sociale" o "attività di addestramento, prova e valutazione degli algoritmi, anche nell'ambito di dispositivi medici, sistemi di IA e applicazioni di sanità digitale, che contribuiscono alla sanità pubblica o alla sicurezza sociale". EDPB e GEPD sono del parere che la proposta dovrebbe delimitare ulteriormente tali finalità e circoscrivere i casi in cui vi è un collegamento sufficiente alla salute pubblica e/o alla sicurezza sociale. Ciò sarà essenziale al fine di conseguire un equilibrio che tenga adeguatamente conto degli obiettivi perseguiti dalla proposta e dalla protezione dei dati personali degli interessati coinvolti in tale trattamento.

Inoltre l'articolo 34, paragrafo 1, della proposta contempla tipi diversi di uso secondario, che rientrerebbero in categorie diverse di motivi di eccezione previsti dall'articolo 9, paragrafo 2, GDPR. Tuttavia EDPB e GEPD ritengono che ciò non si rispecchi nei criteri in base ai quali gli organismi responsabili dell'accesso ai dati sanitari dovrebbero valutare e decidere in merito alle domande di accesso ai dati (articolo 45 della proposta) al fine di rilasciare un'autorizzazione di accesso ai dati (articolo 46 della proposta). A tal fine EDPB e GEPD sottolineano che i criteri previsti al riguardo dall'articolo 46 della proposta si limitano alle disposizioni e ai principi della proposta stessa e mancano di chiarezza circa il modo in cui tali disposizioni si riferiscono ai principi e alle disposizioni di cui al GDPR, in particolare all'articolo 9, paragrafo 2, di tale regolamento.

In relazione al capo V, EDPB e GEPD riconoscono che l'infrastruttura per lo scambio di dati sanitari elettronici prevista nella proposta in questione sullo spazio europeo dei dati sanitari non mira in alcun modo a istituire (né potrebbe determinare l'istituzione di) una banca dati centrale dell'UE di dati sanitari e faciliterà solo lo scambio di tali dati sanitari da banche dati decentralizzate. Tuttavia, in ragione della grande quantità di dati che verrebbero trattati, della loro natura altamente sensibile, del rischio di accesso illecito e della necessità di garantire pienamente un controllo efficace su tali dati, EDPB e GEPD chiedono di aggiungere alla proposta in questione una disposizione che richiederebbe la conservazione dei dati sanitari elettronici personali nell'UE/nello Spazio economico europeo (SEE), fatti salvi ulteriori trasferimenti in conformità al capo V GDPR.

Infine, per quanto riguarda il modello di governance creato dalla proposta, occorre adeguare attentamente i compiti e le competenze dei nuovi enti pubblici, tenendo conto in particolare dei compiti e delle competenze delle autorità nazionali di controllo, di EDPB e GEPD nel settore del trattamento dei dati personali (sanitari). Dovrebbe essere evitata una sovrapposizione di competenze e dovrebbero essere specificati i campi e le prescrizioni per la cooperazione.

Il comitato europeo per la protezione dei dati e il Garante europeo della protezione dei dati

visto l'articolo 42, paragrafo 2, del regolamento (UE) 2018/1725, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE,

visto l'accordo SEE, in particolare l'allegato XI e il protocollo 37, modificati dalla decisione del comitato misto SEE n. 154/2018 del 6 luglio 2018,

HANNO ADOTTATO IL SEGUENTE PARERE CONGIUNTO

1 CONTESTO

1. La proposta di regolamento del Parlamento europeo e del Consiglio sullo spazio europeo dei dati sanitari ("la proposta") contribuirà a realizzare la visione della Commissione in merito alla trasformazione digitale dell'UE entro il 2030[1].

2. Il comitato europeo per la protezione dei dati ("EDPB") e il Garante europeo della protezione dei dati ("GEPD") osservano che, secondo la Commissione, la proposta "*aiuta le persone ad assumere il controllo dei propri dati sanitari; sostiene l'uso dei dati sanitari per migliorare l'erogazione dell'assistenza sanitaria, la ricerca, l'innovazione e l'elaborazione delle politiche; consente all'UE di sfruttare appieno le potenzialità offerte da uno scambio, utilizzo e riutilizzo sicuri dei dati sanitari.*"[2].

3. Come spiegato nella relazione, la proposta è in linea con gli obiettivi generali dell'UE. Tra tali obiettivi figurano la costruzione di un'Unione europea della salute più forte, l'attuazione del pilastro europeo dei diritti sociali, il miglioramento del funzionamento del mercato interno, la promozione di sinergie con l'agenda del mercato interno digitale dell'UE e la realizzazione di un ambizioso programma di

[1] Relazione, pag. 3.
[2] https://ec.europa.eu/health/ehealth-digital-health-and-care/european-health-data-space_it.

ricerca e innovazione. Inoltre la proposta fornirà un'importante serie di elementi che contribuiranno alla formazione dell'Unione europea della salute, incoraggiando l'innovazione e la ricerca e gestendo meglio le future crisi sanitarie.

2 AMBITO DI APPLICAZIONE DEL PARERE

4. Il 3 maggio 2022 la Commissione ha pubblicato la proposta di regolamento del Parlamento europeo e del Consiglio sullo spazio europeo dei dati sanitari ("la proposta").

5. Il 4 maggio 2022 la Commissione ha chiesto un parere congiunto di EDPB e GEPD ("il parere") sulla proposta, a norma dell'articolo 42, paragrafo 2, del regolamento (UE) 2018/1725[3] ("EUDPR").

6. La proposta è di particolare rilevanza per la tutela dei diritti e delle libertà fondamentali delle persone in relazione al trattamento dei loro dati personali. L'ambito di applicazione del parere è limitato agli aspetti della proposta relativi ai dati personali e che contemplano gli stessi, i quali costituiscono uno dei pilastri principali della proposta.

7. EDPB e GEPD accolgono con favore la relazione della proposta nella quale si afferma che "*[c]onsiderando che un volume sostanziale di dati elettronici a cui si deve accedere nello spazio europeo dei dati sanitari è costituito da dati sanitari personali riguardanti persone fisiche nell'UE, la proposta è concepita in piena conformità non solo con l'RGPD ma anche con il regolamento (UE) 2018/1725 (regolamento sulla protezione dei dati nell'ambito delle istituzioni UE)".*

8. Analogamente EDPB e GEPD sottolineano che è necessario garantire e sostenere il rispetto e l'applicazione dell'*acquis* dell'UE nel settore della protezione dei dati. Quando i dati personali sono coinvolti nel contesto della proposta, è essenziale evitare chiaramente nel testo giuridico della proposta qualsiasi incoerenza e possibile conflitto con il regolamento generale sulla protezione dei dati[4] ("GDPR"), la direttiva e-privacy[5] e l'EUDPR. Questo non solo ai fini della certezza del diritto, ma anche per evitare che la proposta abbia l'effetto di mettere a rischio, direttamente o indirettamente, i diritti fondamentali al rispetto della vita privata e alla protezione dei dati di carattere personale stabiliti dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea ("Carta") e dall'articolo 16 del trattato sul funzionamento dell'Unione europea (TFUE).

9. Dato che la proposta, come ulteriormente spiegato nel parere, solleva diverse preoccupazioni in merito alla protezione dei diritti fondamentali al rispetto della vita privata e alla protezione dei dati di carattere personale, il presente parere non mira a fornire un elenco esaustivo di tutte le questioni, né a fornire sempre proposte alternative di suggerimenti di formulazione. Il presente parere mira

[3] Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39).
[4] 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, pag. 1).
[5] 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).

piuttosto ad affrontare le principali criticità della proposta, in relazione al rispetto della vita privata e alla protezione dei dati.

3 VALUTAZIONE

3.1 Osservazioni generali

10. EDPB e GEPD riconoscono l'obiettivo della proposta di ampliare l'uso dei dati sanitari elettronici per fornire assistenza sanitaria alla persona dalla quale tali dati sono stati raccolti ("uso primario") e per migliorare la ricerca, l'innovazione, la definizione delle politiche, la sicurezza dei pazienti, la medicina personalizzata, le statistiche ufficiali o le attività normative ("uso secondario"). EDPB e GEPD riconoscono altresì l'obiettivo della proposta di migliorare il funzionamento del mercato interno stabilendo un quadro giuridico uniforme per quanto riguarda lo sviluppo, la commercializzazione e l'uso di sistemi di cartelle cliniche elettroniche.

11. Tuttavia EDPB e GEPD sottolineano che la protezione dei dati personali è un elemento integrante della fiducia che le persone e le organizzazioni dovrebbero avere nello sviluppo dell'economia digitale[6] e nell'accesso a un'assistenza sanitaria equa, in particolare nel contesto del trattamento dei dati sanitari nel quadro dello spazio europeo dei dati sanitari.

12. A tale proposito EDPB e GEPD sottolineano che il successo dello spazio europeo dei dati sanitari dipenderà da una solida base giuridica per il trattamento in linea con la normativa UE in materia di protezione dei dati, dall'istituzione di un solido meccanismo di governance dei dati e da garanzie efficaci per i diritti e gli interessi delle persone fisiche che siano pienamente conformi al GDPR. Dovrebbero essere fornite garanzie sufficienti in merito a una gestione lecita, responsabile ed etica ancorata ai valori dell'UE, compreso il rispetto dei diritti fondamentali. A questo proposito, EDPB e GEPD ritengono che lo spazio europeo dei dati sanitari dovrebbe fungere da esempio di trasparenza, responsabilizzazione effettiva e giusto equilibrio tra gli interessi dei singoli interessati e l'interesse comune della società nel suo insieme.

13. Nei capitoli che seguono del presente parere, EDPB e GEPD forniranno raccomandazioni su come rendere le disposizioni pertinenti della proposta non solo conformi al quadro giuridico dell'UE in materia di protezione dei dati, ma anche allineate con l'interpretazione corrente della giurisprudenza applicabile della Corte di giustizia dell'Unione europea ("la Corte"). Data l'ampia portata dei diritti e degli obblighi previsti nella proposta in relazione all'accesso, all'uso e alla condivisione di categorie particolari di dati personali come nel caso dei dati sanitari, riferimenti generali al GDPR e all'EUDPR potrebbero non essere sufficienti. A tale proposito, EDPB e GEPD ritengono che vi possa essere il rischio di interpretare erroneamente le disposizioni chiave relative alla protezione dei dati il che, a sua volta, potrebbe portare a un abbassamento del livello di protezione attualmente riconosciuto agli interessati ai sensi del quadro giuridico dell'UE esistente in materia di protezione dei dati (GDPR, EUDPR e direttiva e-privacy). Di conseguenza EDPB e GEPD ritengono necessarie ulteriori specifiche, come verrà dettagliato nel seguito del presente parere.

[6] Parere Congiunto sull'atto sulla governance dei dati.

14. EDPB e GEPD rilevano positivamente che la proposta mira altresì a contribuire ad attenuare l'attuale frammentazione delle norme applicabili al trattamento dei dati sanitari e alla ricerca scientifica. Allo stesso tempo, EDPB e GEPD sollevano dubbi in merito alla piena compatibilità di talune disposizioni dei capi II e IV della proposta (in particolare l'accesso da parte di professionisti sanitari a dati sanitari elettronici personali soggetti a limitazioni, la registrazione sistematica dei dati da parte di professionisti sanitari o il trattamento di risultati imprevisti da parte di organismi responsabili dell'accesso ai dati sanitari nei confronti di persone fisiche) con il diritto degli Stati membri nel settore della sanità elettronica, in assenza di una competenza legislativa generale dell'UE in materia di armonizzazione in questo settore. A tale proposito, occorre ricordare che, ai sensi dell'articolo 168 TFUE, l'azione dell'Unione deve incoraggiare la cooperazione tra gli Stati membri nei settori della sanità pubblica e, ove necessario, appoggiare la loro azione integrando la politica nazionale, rispettando le responsabilità degli Stati membri per la definizione della loro politica sanitaria e per l'organizzazione e la fornitura di servizi sanitari e di assistenza medica.

3.2 Interazione della proposta con la normativa UE in materia di protezione dei dati

15. EDPB e GEPD accolgono con favore il considerando 4 della proposta, secondo il quale "*[i]l trattamento di dati sanitari elettronici personali è soggetto alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio e, per le istituzioni e gli organi dell'Unione, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio. I riferimenti alle disposizioni del regolamento (UE) 2016/679 dovrebbero essere intesi anche come riferimenti alle corrispondenti disposizioni del regolamento (UE) 2018/1725 per le istituzioni e gli organi dell'Unione, se del caso*".

16. Inoltre, secondo la relazione, la proposta si fonda sugli articoli 16 e 114 del trattato sul funzionamento dell'Unione europea (TFUE). Alla luce della proposta, mentre l'articolo 114 TFUE mira a migliorare il funzionamento del mercato interno mediante misure relative al ravvicinamento delle norme nazionali, la proposta mira ad ampliare l'uso dei dati sanitari elettronici rafforzando nel contempo i diritti derivanti dall'articolo 16 TFUE.

17. A questo proposito, EDPB e GEPD, in linea con la giurisprudenza della Corte, sottolineano che l'articolo 16 TFUE fornisce una base giuridica adeguata quando la protezione dei dati personali è una delle finalità o delle componenti essenziali delle norme adottate dal legislatore dell'Unione[7]. Inoltre EDPB e GEPD ricordano che l'applicazione dell'articolo 16 TFUE comporta altresì la necessità di garantire un controllo indipendente per il rispetto delle prescrizioni in materia di trattamento dei dati personali, come previsto anche dall'articolo 8 della Carta[8].

18. In effetti, con riferimento al punto espresso sul controllo indipendente, EDPB e GEPD sottolineano che, secondo il considerando 43 della proposta, le autorità di controllo dovrebbero essere incaricate dell'applicazione delle norme del GDPR e dell'EUDPR con particolare riguardo al trattamento di dati personali per usi secondari nel contesto del capo IV della proposta. A questo proposito EDPB e GEPD raccomandano di inserire una disposizione corrispondente nel dispositivo del testo.

[7] Parere della Corte del 26 luglio 2017, PNR Canada, Parere procedura 1/15, ECLI:EU:C:2017:592, punto 96.
[8] Legge sull'intelligenza artificiale.

19. Per quanto riguarda il ricorso all'articolo 16 TFUE come base giuridica (una delle due[9]) della proposta, EDPB e GEPD riconoscono che l'**obiettivo** della proposta è specificare "ulteriori disposizioni e garanzie giuridicamente vincolanti[10]" in relazione alla protezione dei dati sanitari. Tali disposizioni sono considerate "ulteriori" rispetto a quelle del GDPR. La proposta prevede "prescrizioni e norme specifiche"[11] che sono adattate al trattamento di dati sanitari elettronici e mirano a "concretizza[re] la possibilità offerta dall'RGPD di mettere a punto una normativa dell'UE per varie finalità"[12].

20. Per quanto concerne il **contenuto** della proposta**,** EDPB e GEPD desiderano formulare due osservazioni generali.

21. Innanzitutto la proposta contiene prevalentemente norme sul trattamento di dati personali (sanitari), tanto per uso primario quanto per uso secondario. Visto l'impatto di tali disposizioni sul baricentro generale della proposta, EDPB e GEPD convengono che il contenuto della proposta rende l'articolo 16 TFUE una base giuridica necessaria. Ciò non pregiudica le osservazioni di cui al presente parere circa l'interazione di diverse disposizioni della proposta con quelle del GDPR, un'interazione che richiede decisamente ulteriori chiarimenti e, talvolta, ulteriori riflessioni e rielaborazioni, come illustrato più avanti nel presente parere.

22. EDPB e GEPD rilevano inoltre che, secondo il considerando 37, la proposta mira a mettere a disposizione diritto dell'Unione avvalendosi delle eccezioni di cui all'articolo 9, paragrafo 2, lettera g), i) e j), GDPR. EDPB e GEPD osservano altresì che, per l'uso secondario di dati sanitari, la proposta crea l'obbligo per i titolari dei dati ai sensi dell'articolo 6, paragrafo 1, lettera c), GDPR di comunicare i dati agli organismi responsabili dell'accesso ai dati sanitari. Allo stesso tempo, EDPB e GEPD comprendono che la proposta non mira a creare una base giuridica per i richiedenti accesso ai dati in relazione all'articolo 6 GDPR né a modificare i requisiti in materia di informazione ai sensi del GDPR o della direttiva e-privacy, né di alterare i diritti ivi stabiliti.

23. In secondo luogo, EDPB e GEPD rilevano che la proposta contiene almeno una deroga esplicita a una disposizione del GDPR: l'articolo 38, paragrafo 2, della proposta esenta infatti alcuni soggetti (gli organismi responsabili dell'accesso ai dati sanitari) dall'applicazione delle disposizioni di cui all'articolo 14 GDPR riguardante le informazioni da fornire agli interessati. EDPB e GEPD ritengono che tale esenzione pregiudichi la possibilità per gli interessati di esercitare un controllo efficace sui propri dati personali anziché rafforzarlo e sembra quindi essere in contrasto con l'obiettivo di cui all'articolo 1, paragrafo 2, lettera a), della proposta. Inoltre EDPB e GEPD si chiedono se sia necessario e giustificato introdurre una limitazione del diritto di informazione come ulteriormente spiegato ai punti 26, 34, 96 e 97 del presente parere, anche in considerazione dell'articolo 23 GDPR.

24. Più in generale, EDPB e GEPD mettono in guardia contro disposizioni legislative che prevedono deroghe ai compiti e ai poteri delle autorità di controllo della protezione dei dati e alle norme generalmente applicabili del GDPR in conformità con l'articolo 8 della Carta. Tale normativa incide inevitabilmente e, in definitiva, può compromettere, nel tempo, la centralità delle norme orizzontali

[9] GEPD ed EDPB, in linea con i loro mandati, non tratteranno nel presente parere la questione della giustificazione del ricorso a una doppia base giuridica e si limiteranno a considerazioni relative al ricorso all'articolo 16 TFUE.
[10] Relazione della proposta, pag. 7.
[11] Ibidem.
[12] Ibidem.

adottate ai sensi dell'articolo 16 TFUE. Le autorità di controllo indipendenti dovrebbero avere il compito di vigilare sulla proposta per quanto riguarda il trattamento dei dati personali.

25. In ogni caso, EDPB e GEPD si chiedono se una limitazione del diritto all'informazione sia necessaria e giustificata in questo contesto. In effetti, tanto l'articolo 14, paragrafo 5, lettera b) quanto l'articolo 14, paragrafo 5, lettera c), GDPR esentano i titolari del trattamento dal rispettare l'articolo 14, GDPR in taluni casi, in particolare nella misura in cui 1) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento[13] e 2) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato. Nella misura in cui la proposta sullo spazio europeo dei dati sanitari prevede espressamente l'ottenimento o la divulgazione di dati personali, si dovrebbe piuttosto valutare se la proposta contenga garanzie adeguate a tutelare gli interessi legittimi degli interessati.

26. Infine, EDPB e il GEPD osservano che, sebbene la proposta tratti anche le applicazioni per il benessere e altre applicazioni di sanità digitale, la direttiva e-privacy non è inclusa nel suo articolo 1, paragrafo 4. Sebbene mettano in dubbio l'inclusione di tali applicazioni nell'ambito di applicazione del capo IV della proposta, come verrà spiegato nel prossimo capitolo, EDPB e GEPD raccomandano di includere un riferimento alla direttiva e-privacy, qualora tali applicazioni costituiscano comunque parte della proposta.

27. Inoltre l'articolo 1, paragrafo 4, della proposta dovrebbe fare riferimento anche all'EUDPR e le disposizioni pertinenti di tale atto dovrebbero altresì essere individuate esplicitamente in tutta la proposta[14]. Riferimenti espliciti ai pertinenti articoli dell'EUDPR nei termini di attuazione della proposta sembrano più che giustificati, innanzitutto dato che la Commissione agirà in veste di responsabile del trattamento per i dati sanitari elettronici comunicati tramite "MyHealth@EU" (articolo 12, paragrafo 7, della proposta), in secondo luogo, dato che le istituzioni, gli organi e gli organismi dell'Unione possono avere accesso regolare ai dati sanitari elettronici (considerando 41 della proposta) e, in terzo luogo, in considerazione del fatto che i dati detenuti dalle istituzioni dell'Unione possono essere messi a disposizione anche per un uso secondario (considerando 46 della proposta).

3.3 Interazione della proposta con l'atto sulla governance dei dati, la normativa sui dati e la legge sull'intelligenza artificiale

28. EDPB e GEPD osservano che, in linea con l'articolo 1, paragrafo 4, della proposta, "*[i]l [...] regolamento lascia impregiudicati gli altri atti giuridici dell'Unione relativi all'accesso ai dati sanitari elettronici, alla loro condivisione o al loro uso secondario o le prescrizioni relative al trattamento dei dati in relazione*

[13] In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni.
[14] Ai sensi del considerando 4 della proposta, i riferimenti alle disposizioni del GDPR dovrebbero essere intesi anche come riferimenti alle corrispondenti disposizioni dell'EUDPR. Sebbene l'obiettivo del considerando 4 sia chiaro, EDPB e GEPD raccomandano vivamente che le disposizioni pertinenti dell'EUDPR siano individuate esplicitamente nei termini di attuazione della proposta in quanto tale.

ai dati sanitari elettronici, in particolare i regolamenti (UE) 2016/679, (UE) 2018/1725, [...] [Atto sulla governance dei dati (COM(2020) 767 final)] e [...] [normativa sui dati (COM(2022) 68 final)]". Inoltre, in linea con l'articolo 1, paragrafo 5, della proposta, il "*[...] regolamento lascia impregiudicati i regolamenti (UE) 2017/745 e [...] [legge sull'intelligenza artificiale (COM(2021) 206 final)] per quanto riguarda la sicurezza dei dispositivi medici e dei sistemi di intelligenza artificiale (IA) che interagiscono con i sistemi di cartelle cliniche elettroniche*".

29. Pur accogliendo favorevolmente il riferimento esplicito al fatto che la proposta non pregiudica l'atto sulla governance dei dati, la normativa sui dati e la legge sull'intelligenza artificiale, EDPB e GEPD ritengono che l'interazione specifica della proposta con le suddette iniziative, facenti parte del pacchetto digitale, nonché il regolamento sui dispositivi medici[15], dovrebbe essere affrontata meglio. Per illustrare questo punto e soltanto a titolo esemplificativo, la proposta introduce una definizione di "titolare dei dati" all'articolo 2, paragrafo 2, lettera y), che potrebbe non essere coerente con la definizione di titolare dei dati di cui all'atto sulla governance dei dati e alla normativa sui dati. Ciò potrebbe comportare incertezza del diritto su quali soggetti rientrerebbero in tale definizione, nonostante ciò costituisca un aspetto centrale della proposta, dato che determinerebbe, in modo cruciale, quali soggetti saranno tenuti a rispettare l'obbligo di rendere disponibili i dati sanitari elettronici per un uso secondario.

30. EDPB e GEPD rilevano altresì che l'obiettivo generale della proposta è garantire che le persone fisiche nell'UE dispongano di un controllo maggiore sui loro dati sanitari elettronici, che non può essere ottenuto se l'interazione tra le normative pertinenti non è individuata in maniera chiara. La certezza del diritto è fondamentale non soltanto per assicurare che i diversi portatori di interessi si sentano sicuri nell'agire nel contesto del nuovo quadro, ma anche per garantire i diritti delle persone fisiche. Di conseguenza EDPB e GEPD raccomandano di chiarire ulteriormente l'interazione della proposta con le iniziative e gli strumenti giuridici summenzionati.

4 DISPOSIZIONI GENERALI (CAPO I)

4.1 Articolo 1: oggetto e ambito di applicazione della proposta

31. EDPB e GEPD accolgono con favore il fatto che la proposta miri, tra l'altro, a rafforzare i diritti delle persone fisiche in relazione alla disponibilità e al controllo dei loro dati sanitari elettronici.

32. EDPB e GEPD sono consapevoli che la pandemia di COVID-19 ha notevolmente accelerato il ricorso a dispositivi medici, applicazioni per il benessere o dispositivi indossabili tra la popolazione generale. Tuttavia questo tipo di tecnologia genera un'enorme quantità di dati, spesso categorie particolari di dati personali, e può essere altamente invasiva. Più che tenere traccia delle azioni e delle decisioni delle persone, è ora possibile tracciare i corpi, le menti e le emozioni delle persone a un livello tale che persino le persone stesse potrebbero non essere in grado di fare. Tali dati possono quindi essere utilizzati per prevedere le azioni delle persone e manipolare il loro comportamento, anche a livello di gruppo.

[15] Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio (GU L 117 del 5.5.2017, pag. 1).

33. EDPB e GEPD rilevano che, come stabilito all'articolo 1, paragrafo 2, lettera a), della proposta, il primo obiettivo della proposta è rafforzare i diritti delle persone fisiche in relazione alla disponibilità e al controllo dei loro dati sanitari elettronici. Allo stesso tempo, EDPB e GEPD rilevano altresì che, a differenza dell'uso primario, per il quale la proposta consente alle persone fisiche di limitare l'accesso ai propri dati personali, la stessa opzione non è concessa per quanto concerne l'uso secondario dei dati. Inoltre, ai sensi dell'articolo 38, paragrafo 2, della proposta, "*[g]li organismi responsabili dell'accesso ai dati sanitari non sono tenuti a fornire a ciascuna persona fisica le informazioni specifiche di cui all'articolo 14 del regolamento (UE) 2016/679 in merito all'uso dei loro dati per progetti sottoposti a un'autorizzazione ai dati* [...]". EDPB e GEPD sottolineano che il diritto all'informazione e il diritto di opposizione sono indissolubilmente legati. EDPB e GEPD sono del parere che, limitando il diritto all'informazione ai sensi del GDPR, la proposta potrebbe non conseguire gli obiettivi di cui al suo articolo 1, paragrafo 2, lettera a). Infatti, l'approccio prospettato sembra ledere i diritti delle persone fisiche alla vita privata e alla protezione dei dati personali, soprattutto tenendo conto della definizione molto ampia di uso secondario e delle categorie minime di dati elettronici per l'uso secondario introdotte dalla proposta, che non si limitano soltanto alla ricerca scientifica, ma comprendono anche altre finalità, quali l'innovazione.

34. Inoltre EDPB e GEPD rilevano che l'articolo 1, paragrafo 3, lettera a), della proposta prevede che la proposta si applichi "[...] ai *fabbricanti e ai fornitori di* ***sistemi di cartelle cliniche elettroniche*** *e di* ***applicazioni per il benessere*** *immessi sul mercato e messi in servizio nell'Unione e agli utilizzatori di tali prodotti*", mentre l'articolo 33, paragrafo 1, lettere f) e n), della proposta elenca tra le categorie minime di dati elettronici per l'uso secondario i dati sanitari elettronici generati dalla persona, compresi **dispositivi medici, applicazioni per il benessere o altre applicazioni di sanità digitale, nonché dati relativi al benessere e ai comportamenti pertinenti per la salute** (grassetto aggiunto). Innanzitutto si rileva un'incoerenza tra l'ambito di applicazione della proposta e le categorie di dati elencate all'articolo 33, paragrafo 1, lettera f), della stessa: il primo fa riferimento soltanto ai fabbricanti e ai fornitori di sistemi di cartelle cliniche elettroniche e di applicazioni per il benessere, mentre nelle seconde sono compresi altresì dispositivi medici oltre ad applicazioni per il benessere e altre applicazioni di sanità digitale. EDPB e GEPD sono dell'avviso che anche i dispositivi medici rientrino nell'ambito di applicazione della proposta. Di conseguenza, per motivi di chiarezza giuridica, EDPB e GEPD raccomandano di aggiungere i fabbricanti e i fornitori di dispositivi medici all'articolo 1, paragrafo 3, lettera a), della proposta.

35. Inoltre EDPB e GEPD sottolineano che i dati sanitari generati da applicazioni per il benessere e da altre applicazioni di sanità digitale non soddisfano le medesime prescrizioni in termini di qualità dei dati e non presentano le medesime caratteristiche di quelli generati dai dispositivi medici (dato che questi ultimi sono soggetti a norme e normative specifiche esistenti). Occorre altresì rilevare che le applicazioni di sanità digitale possono eventualmente raccogliere dati personali che vanno oltre i dati sanitari: ad esempio la raccolta di informazioni personali concernenti pratiche alimentari e altre abitudini può rivelare indirettamente informazioni particolarmente sensibili quali l'orientamento religioso.

36. In questo contesto, sebbene comprendano la possibile necessità di includere i dispositivi medici nell'ambito di applicazione della proposta, **EDPB e GEPD raccomandano di escludere dall'articolo 33, paragrafo 1, lettere f) e n), della proposta rispettivamente le applicazioni per il benessere e altre applicazioni digitali, nonché i dati relativi al benessere e ai comportamenti pertinenti per la salute**. In caso di conservazione di tali dati, il trattamento per l'uso secondario di dati personali derivanti da applicazioni per il benessere e altre applicazioni digitali dovrebbe essere subordinato al consenso

preventivo ai sensi del GDPR. Inoltre EDPB e GEPD ricordano che tale trattamento può rientrare nell'ambito di applicazione della direttiva 2002/58/CE ("direttiva relativa alla vita privata e alle comunicazioni elettroniche" o "direttiva e-privacy").

37. EDPB e GEPD rilevano che, ai sensi dell'articolo 2, paragrafo 2, della proposta, la definizione di titolare dei dati contempla esplicitamente le istituzioni dell'Unione. Tuttavia **le istituzioni dell'Unione possono agire tanto in veste di titolare del trattamento di dati personali e relativi alla salute (e quindi di titolare dei dati) quanto in qualità di utente di dati personali e relativi alla salute**[16]. Questo aspetto è spiegato al considerando 41 e agli articoli 34, 45 e 48 della proposta. Di conseguenza, e per motivi di certezza del diritto, EDPB e GEPD **raccomandano di chiarire se le istituzioni dell'Unione sono incluse o meno anche nella definizione di utente dei dati**. Infine, EDPB e GEPD ricordano che, dato che le istituzioni, gli organi e gli organismi dell'Unione non sono soggetti a giurisdizioni nazionali, è opportuno fornire specifici chiarimenti in relazione alle sanzioni che possono essere applicate dagli organismi responsabili dell'accesso ai dati sanitari, come previsto dall'articolo 43 della proposta.

4.2 Articolo 2: definizioni

38. EDPB e GEPD rilevano che l'articolo 2 della proposta fornisce definizioni pertinenti per la comprensione del regolamento nel suo complesso. Tuttavia ritengono che diverse definizioni siano molto ampie e si prestino all'interpretazione, circostanza questa che può portare a incertezza del diritto.

39. Innanzitutto l'articolo 2, paragrafo 1, lettera a), della proposta stabilisce che si applicano le **definizioni contenute nel regolamento (UE) 2016/679**. Allo stesso tempo la proposta introduce definizioni nuove e fa riferimento a concetti specifici di cui in altri regolamenti, quali la normativa sui dati. Ad esempio la proposta introduce la definizione di "destinatario dei dati", sebbene tale definizione figuri già all'articolo 4, punto 9, GDPR. Dato che la proposta mira a integrare talune disposizioni del GDPR, per motivi di certezza del diritto EDPB e GEPD raccomandano di spiegare perché sono necessarie definizioni aggiuntive o, nel caso più estremo, in via eccezionale, di individuare le definizioni del GDPR che non si applicano.

40. L'articolo 2, paragrafo 2, lettera a), della proposta definisce i **"dati sanitari elettronici personali"** come i dati relativi alla salute e i dati genetici quali definiti nel GDPR, nonché i dati relativi a determinanti della salute o i dati trattati nell'ambito della prestazione di servizi di assistenza sanitaria, che sono

[16] Le istituzioni, gli organi e gli organismi dell'Unione trattano i dati relativi alla salute principalmente nei contesti seguenti:
1. assunzione (visita medica pre-assunzione);
2. medicina del lavoro (visita medica annuale)/salute e sicurezza sul posto di lavoro;
3. rimborso di spese mediche (regime comune di assicurazione malattia);
4. congedi di malattia (certificati medici) e procedure di invalidità; e
5. svolgimento di un compito assegnato nel contesto della missione delle istituzioni dell'Unione (ad esempio Centro europeo per la prevenzione e il controllo delle malattie e Agenzia europea per i medicinali).

È probabile che i trattamenti di dati sanitari presentino rischi specifici e maggiori per i diritti e le libertà degli interessati, che sono membri del personale, agenti temporanei, agenti contrattuali, esperti nazionali, tirocinanti di tali organi, candidati ai posti di lavoro di cui sopra nonché visitatori presso le istituzioni dell'Unione. Tali rischi sono analoghi a quelli cui gli interessati sono esposti quando i loro dati sanitari sono trattati da titolari del trattamento che non sono istituzioni dell'Unione.

trattati in formato elettronico. A questo proposito, è opportuno sottolineare che il considerando 35 GDPR comprende già le informazioni raccolte nel corso della prestazione di servizi di assistenza sanitaria. Inoltre il considerando 54 della proposta fa riferimento anche ai "determinanti aventi un effetto su tale stato di salute", in particolare nel contesto del trattamento di tali dati relativi alla salute per motivi di interesse pubblico. Per garantire il maggior allineamento possibile con il GDPR, EDPB e GEPD raccomandano di modificare la definizione di cui all'articolo 2, paragrafo 2, lettera a), della proposta per fare semplicemente riferimento ai "dati relativi alla salute e i dati genetici quali definiti nel regolamento (UE) 2016/679, che sono trattati in formato elettronico".

41. Al contrario, l'articolo 2, paragrafo 2, lettera b), della proposta definisce i "**dati sanitari elettronici non personali"** come i dati relativi alla salute e i dati genetici in formato elettronico che non rientrano nella definizione di dato personale di cui all'articolo 4, punto 1, GDPR. A questo proposito, EDPB e GEPD sottolineano nuovamente[17] che la distinzione tra categorie di dati personali e non personali è difficile da applicare nella pratica. Da una combinazione di dati non personali, in effetti, è possibile dedurre o generare dati personali, ossia dati relativi a una persona identificata o identificabile, soprattutto quando i dati non personali sono il risultato dell'anonimizzazione di dati personali e persino di più nel contesto del trattamento di dati sanitari. In questo contesto, EDPB e GEPD prendono atto del rischio di reidentificazione di cui al considerando 64 della proposta e raccomandano di rendere più esplicito il fatto che, in caso di serie di dati miste (nel contesto delle quali i dati personali e non personali sono "legati tra loro in modo inscindibile") si applicano le tutele del GDPR e della proposta in materia di dati sanitari elettronici personali.

42. L'articolo 2, paragrafo 2, lettera d) e l'articolo 2, paragrafo 2, lettera e), della proposta definiscono rispettivamente l'"**uso primario dei dati sanitari elettronici"** e l'"**uso secondario dei dati sanitari elettronici"**. EDPB e GEPD ritengono che tali definizioni possano dar luogo a incertezza del diritto e incoerenza rispetto al GDPR, in particolare per quanto concerne la definizione di uso secondario dei dati sanitari elettronici. In particolare, la seconda parte dell'articolo 2, paragrafo 2, lettera e), della proposta afferma che "*[t]ra i dati utilizzati possono figurare dati [...] elettronici personali originariamente raccolti nel contesto dell'uso primario, ma anche dati [...] elettronici raccolti ai fini dell'uso secondario".* EDPB e GEPD ritengono che, poiché il concetto di "uso secondario dei dati personali" non compare nel GDPR, la seconda parte della definizione di "uso secondario dei dati sanitari elettronici" si discosta dal concetto di "ulteriore trattamento dei dati personali" di cui al GDPR. Quest'ultimo concetto, infatti, è da intendersi in relazione alla finalità per la quale un determinato titolare del trattamento ha originariamente raccolto i dati, a prescindere dagli aspetti qualitativi dei dati stessi. Di conseguenza, EDPB e GEPD raccomandano di correggere tali definizioni alla luce del GDPR, e in particolare di chiarire il collegamento tra la definizione di uso secondario dei dati sanitari elettronici ai sensi della proposta e il concetto di ulteriore uso dei dati personali ai sensi del GDPR, tenendo conto soprattutto del regime speciale già previsto da quest'ultimo regolamento per la ricerca scientifica.

43. L'articolo 2, paragrafo 2, lettera f), della proposta definisce **"interoperabilità**" come "*la capacità delle organizzazioni, nonché delle applicazioni software o dei dispositivi dello stesso fabbricante o di fabbricanti diversi, di interagire tra loro per conseguire obiettivi reciprocamente vantaggiosi, il che comporta lo scambio di informazioni e conoscenze tra tali organizzazioni, applicazioni software o dispositivi, attraverso i processi che essi supportano, senza che sia modificato il contenuto dei dati*". A tale proposito, EDPB e GEPD ritengono che tale definizione possa necessitare di ulteriori chiarimenti

[17] Parere congiunto EDPB- GEPD relativo all'atto sulla governance dei dati, punto 58.

in merito alla sua interazione con le definizioni di interoperabilità già esistenti in altre normative quali l'atto sulla governance dei dati e il regolamento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (regolamento eIDAS).

44. L'articolo 2, paragrafo 2, lettera y), della proposta definisce un **"titolare dei dati"** come "*una persona fisica o giuridica che è un soggetto o un organismo del settore sanitario o dell'assistenza, o che svolge attività di ricerca in relazione a tali settori, nonché le istituzioni, gli organi e gli organismi dell'Unione che hanno il diritto o l'obbligo, conformemente al presente regolamento, al diritto dell'Unione applicabile o alla legislazione nazionale di attuazione del diritto dell'Unione, o, nel caso di dati non personali, mediante il controllo della progettazione tecnica di un prodotto e dei servizi correlati, la capacità, di rendere disponibili determinati dati, anche in termini di registrazione, fornitura, limitazione dell'accesso o scambio*". Come già sottolineato in precedenza al punto 29, si tratta di una definizione fondamentale, ma così ampia da non consentire di individuare chiaramente chi si qualificherebbe come titolare dei dati[1] e di comprendere quale sia l'interazione con la definizione di titolare del trattamento di cui alla normativa sui dati e all'atto sulla governance dei dati. Se non definisce chiaramente chi rientra in detta definizione, tale disposizione può dar luogo a incertezza del diritto in merito a chi è tenuto a rendere i dati disponibili per un uso secondario ai sensi dell'articolo 33, paragrafo 1, e dell'articolo 44 della proposta, una circostanza questa che a sua volta potrebbe compromettere i diritti degli interessati al rispetto della vita privata e alla protezione dei dati. Peraltro detta definizione è in contrasto con l'articolo 3, paragrafo 8, della proposta, che fa riferimento anche al settore della sicurezza sociale, attualmente non ricompreso nella stessa definizione fornita dall'articolo 2, paragrafo 2, lettera y), della proposta. EDPB e GEPD sono pertanto del parere che, ai fini della certezza del diritto, sia importante chiarire tale concetto.

45. L'articolo 2, paragrafo 2, lettera z), della proposta definisce un **"utente dei dati"** come "*una persona fisica o giuridica che ha legalmente accesso ai dati sanitari elettronici personali o non personali ai fini dell'uso secondario*". A questo proposito, EDPB e GEPD ritengono che la sua relazione con la definizione di "destinatario dei dati" ai sensi dell'articolo 2, paragrafo 2, lettera k), della proposta, nonché la definizione di "destinatario" nel GDPR non sia chiara. Tale mancanza di chiarezza si applica anche all'interazione di questa definizione con la nozione di "utente dei dati" nell'atto sulla governance dei dati. Inoltre EDPB e GEPD fanno riferimento alla raccomandazione formulata al punto 37 del presente parere sull'inclusione delle istituzioni dell'Unione in tale definizione. Infine GEPD ed EDPB ritengono che, anziché affermare che una persona giuridica ha legalmente accesso ai dati sanitari elettronici personali, sarebbe più appropriato fare riferimento alla possibilità o meno di effettuare tale accesso e a quali condizioni.

5 USO PRIMARIO DEI DATI SANITARI ELETTRONICI (CAPO II)

46. EDPB e GEPD rilevano che, per quanto concerne l'uso primario dei dati sanitari elettronici, così come previsto nella proposta, è necessario raggiungere un equilibrio tra l'agevolazione della disponibilità delle registrazioni elettroniche, a livello nazionale, di UE o internazionale, e le ripercussioni sui diritti e sulle libertà delle persone in generale, nonché sui diritti di cui al GDPR. EDPB e GEPD ritengono che, ai fini del conseguimento di tale obiettivo, il colegislatore dovrebbe tenere conto degli aspetti della proposta trattati di seguito.

47. Innanzitutto EDPB e GEPD rilevano che l'articolo 3 della proposta fa riferimento ai diritti delle persone fisiche in relazione all'uso primario dei loro dati sanitari elettronici personali[18]. EDPB e GEPD nutrono forti preoccupazioni in merito all'interazione di tali diritti di nuova introduzione con quelli previsti dagli articoli da 15 a 22 GDPR. In particolare EDPB e GEPD sono preoccupati per la sovrapposizione dei diritti previsti nella proposta con quelli previsti nel GDPR e per il rischio di incertezza del diritto che ciò può comportare nei confronti degli interessati. Di conseguenza, per motivi di certezza del diritto, EDPB e GEPD esortano il colegislatore a chiarire la relazione tra tali diritti e a garantire che non limitino (direttamente o indirettamente) la portata dei diritti delle persone ai sensi della legislazione dell'UE in materia di protezione dei dati.

48. L'articolo 3 della proposta introduce il diritto di accesso immediato e il diritto di dare accesso o richiedere la trasmissione di dati a destinatari di loro scelta, nonché il diritto di limitare l'accesso dei professionisti sanitari alla totalità o a parte dei loro dati sanitari elettronici e di ottenere informazioni sui prestatori di assistenza sanitaria e sui professionisti sanitari che hanno avuto accesso ai loro dati sanitari elettronici nell'ambito dell'assistenza sanitaria. Come affermato al considerando 1 della proposta, "*[i]l presente regolamento ha lo scopo di istituire lo spazio europeo dei dati sanitari (European Health Data Space, EHDS) al fine di migliorare l'accesso delle persone fisiche ai loro dati sanitari elettronici personali e il loro controllo su tali dati nel contesto dell'assistenza sanitaria (uso primario dei dati sanitari elettronici) […]*". Il considerando 6 della proposta spiega che lo spazio europeo dei dati sanitari si basa sui diritti di cui al GDPR degli interessati e li sviluppa ulteriormente, sostenendo nel contempo l'attuazione coerente di tali diritti applicati ai dati sanitari elettronici.

49. In tale contesto, EDPB e GEPD sottolineano che, al momento della stesura del presente parere, non è stata effettuata alcuna valutazione d'impatto sulla protezione dei dati[19] in relazione alla proposta. Di conseguenza non ha avuto luogo una valutazione del modo in cui le modifiche previste possano incidere sui diritti e sulle libertà degli interessati, nonché del rischio che ne deriva.

50. Inoltre EDPB e GEPD accolgono con favore il fatto che la proposta faccia riferimento ai diritti di cui al GDPR (ad esempio il diritto di accesso gratuito e il diritto di ottenere una copia dei dati)[20]. Tuttavia EDPB e GEPD rilevano che la descrizione dei diritti così come fornita nella proposta non è coerente con quella di cui al GDPR. Come accennato in precedenza, ciò può comportare incertezza del diritto negli interessati che potrebbero non essere in grado di distinguere tra i due tipi di diritti. A tal fine, così come al fine di evitare complessità nell'attuazione pratica, EDPB e GEPD esortano il colegislatore

[18] Ad esempio per quanto concerne il nuovo diritto degli interessati di limitare l'accesso dei professionisti sanitari alla totalità o a parte dei loro dati sanitari elettronici stabilito dall'articolo 3, paragrafo 9, della proposta, non è chiaro se le norme e le garanzie specifiche che devono essere stabilite dal diritto degli Stati membri secondo le medesime disposizioni devono rispettare le norme previste dall'articolo 18, paragrafi 2 e 3, GDPR in materia di diritto alla limitazione del trattamento dei dati.

[19] Per quanto concerne questa questione la proposta è accompagnata da una relazione sulla valutazione d'impatto (documento di lavoro dei servizi della Commissione - doc. 8751/22 ADD 3, del 6 maggio 2022), che contiene soltanto una panoramica generale di tre opzioni strategiche per quanto concerne l'impatto sui diritti fondamentali. Ciò non costituisce una valutazione d'impatto sulla protezione dei dati ai sensi del GDPR, che sarebbe indispensabile per disporre di un'analisi approfondita della valutazione dei rischi che un trattamento di categorie speciali di dati su larghissima scala comporterebbe, così come per prevedere le necessarie misure di attenuazione e garanzie.

[20] Cfr. ad esempio l'articolo 15, paragrafi 1 e 3, GDPR, in merito all'esistenza del diritto di accesso e del diritto ad ottenere copia dei dati, e l'articolo 12, paragrafo 5, GDPR, che prevede l'esercizio gratuito di tali diritti.

a garantire chiarezza giuridica in merito all'interazione tra i diritti dell'interessato introdotti dalla proposta e le disposizioni generali contenute nel GDPR in merito ai diritti degli interessati.

51. Ciò è ancor più pertinente per garantire che gli interessati con capacità limitate di accedere ai servizi digitali e di usufruirne non siano tenuti a fare affidamento su terzi per esercitare i loro diritti fondamentali e, di conseguenza, non siano tenuti a esporre la propria vita privata e i propri dati personali ad altre persone fisiche per poter richiedere l'accesso ai loro dati, ai sensi dell'articolo 3, paragrafo 5, lettera b), della proposta.

52. EDPB e GEPD rilevano che la rappresentanza di un interessato nell'esercizio dei suoi diritti alla protezione dei dati deve soddisfare determinati requisiti di certezza del diritto. Il concetto di autorizzazione introdotto dall'articolo 3, paragrafo 5, della proposta sui servizi generali di delega per l'accesso potrebbe non essere sufficiente a garantire che gli interessati non siano in alcun modo costretti a fornire ad altre persone fisiche di loro scelta l'accesso ai loro dati per loro conto[21].

53. Inoltre EDPB e GEPD sottolineano che un concetto così ampio di autorizzazione senza alcuna garanzia apre le porte a un possibile uso abusivo del diritto di accesso ai dati sanitari elettronici. Infatti la prescrizione che prevede che un rappresentante sia soltanto una persona fisica non impedisce necessariamente l'accesso ai dati da parte di imprese private. Pertanto, al fine di prevenire tali possibili abusi, EDPB e GEPD raccomandano di istituire garanzie supplementari che accompagnino tale meccanismo di autorizzazione.

54. Per quanto concerne il diritto alla rettifica di cui all'articolo 3, paragrafo 7, della proposta, EDPB e GEPD rilevano che non è chiaro dalla proposta chi sarà il soggetto competente per garantire la rettifica dei dati. Ciò è problematico, tenendo conto del fatto che in questo contesto esistono molteplici fonti e destinatari di dati personali, a livello nazionale, ma anche a livello di UE e persino a livello internazionale. EDPB e GEPD sottolineano che, ai sensi del GDPR, tale obbligo ricade sul titolare del trattamento. Tuttavia, poiché, in questo contesto, vi sono diversi titolari del trattamento che contribuiscono con dati sanitari elettronici da mettere a disposizione, EDPB e GEPD invitano i colegislatori a chiarire nella proposta come sarà garantito nella pratica il rispetto del diritto di rettifica.

55. EDPB e GEPD osservano altresì che l'articolo 3, paragrafo 8, della proposta prevede che le persone fisiche debbano avere il diritto di concedere l'accesso ai loro dati sanitari elettronici a un destinatario dei dati di loro scelta del settore sanitario o della sicurezza sociale o di chiedere a un titolare dei dati del settore sanitario o della sicurezza sociale di trasmettere i loro dati sanitari elettronici a un destinatario dei dati di loro scelta del settore sanitario o della sicurezza sociale, immediatamente, gratuitamente e senza ostacoli da parte del titolare dei dati o dei fabbricanti dei sistemi utilizzati da tale titolare. A tale proposito EDPB e GEPD sottolineano che il destinatario dei dati deve essere adeguatamente identificato dal sistema, anche dimostrando che il soggetto che riceve i dati appartiene al settore sanitario o della sicurezza sociale.

56. EDPB e GEPD ritengono inoltre che, in linea con l'autodeterminazione dell'interessato, nel decidere a quale destinatario dei dati saranno resi disponibili i suoi dati sanitari elettronici ai sensi dell'articolo 3,

[21] Occorre tenere conto del fatto che in alcuni Stati membri ciò può essere fatto legalmente soltanto ricorrendo a un notaio, indipendentemente dal fatto che la persona che accede sia un tutore legale o meno. È importante ricordare che il motivo dell'intervento di un notaio risiede nella necessità di garantire una libera indicazione delle intenzioni degli interessati.

paragrafo 8, della proposta, quest'ultimo dovrebbe garantire che l'interessato possa decidere altresì quali dati devono essere trasmessi, in maniera analoga rispetto a quanto previsto dalla proposta al suo articolo 3, paragrafo 9. In particolare, EDPB e GEPD sottolineano che la proposta dovrebbe prevedere la possibilità che siano trasmessi soltanto i dati necessari alla finalità in questione, richiedendo l'adozione di misure tecniche di tutela della vita privata fin dalla progettazione, al fine di rispettare il principio della minimizzazione dei dati.

57. Infine EDPB e GEPD osservano che, sebbene l'articolo 3, paragrafo 8, della proposta introduca un nuovo diritto degli interessati, ossia la possibilità di trasmettere i propri dati sanitari elettronici a un destinatario dei dati di loro scelta, detta disposizione non stabilisce un corrispondente obbligo esplicito per il titolare dei dati a procedere in tal senso. Dato che, in linea di principio, l'articolo 9, paragrafo 1, GDPR non consente il trattamento di dati personali relativi alla salute, nonché di dati genetici, fatto salvo il caso in cui si applichi una delle esenzioni di cui all'articolo 9, paragrafo 2, del medesimo regolamento, EDPB e GEPD raccomandano al colegislatore di allineare l'articolo 3, paragrafo 8, della proposta all'articolo 6 e all'articolo 9, paragrafo 2, GDPR nonché di chiarire l'interazione di tale disposizione con le possibili ulteriori condizioni, comprese le limitazioni, concernenti il trattamento di dati relativi alla salute o genetici che gli Stati membri potrebbero aver mantenuto o introdotto ai sensi dell'articolo 9, paragrafo 4, GDPR.

58. EDPB e GEPD accolgono con favore la disposizione di cui all'articolo 3, paragrafo 10, della proposta, in quanto ciò garantisce agli interessati un controllo efficace sui loro dati personali, consentendo loro di individuare potenziali accessi illeciti ai propri dati sanitari. Ciò nonostante essi ritengono che non sia chiaro se il diritto di ottenere informazioni sia da esercitarsi mediante una procedura di notifica automatica ogniqualvolta vi sia accesso ai dati o sia possibile soltanto su richiesta. EDPB e GEPD ritengono che la prima opzione sia la soluzione più adeguata per conferire potere all'interessato. Pertanto EDPB e GEPD raccomandano che si tratti di un aspetto che i colegislatori dovrebbero prendere in considerazione e quindi chiarito di conseguenza.

59. In relazione all'articolo 4, paragrafo 1, della proposta, EDPB e GEPD rilevano che i professionisti sanitari: a) hanno accesso ai dati sanitari elettronici delle persone fisiche in cura presso di loro, indipendentemente dallo Stato membro di affiliazione e dallo Stato membro di cura; e b) garantiscono che i dati sanitari elettronici personali delle persone fisiche che curano siano aggiornati con informazioni relative ai servizi sanitari prestati. Al riguardo, poiché EDPB e GEPD rilevano che l'accesso ai dati sanitari elettronici personali potrebbe essere già stato affrontato e disciplinato a livello nazionale, raccomandano ai colegislatori di chiarire il rapporto tra tale disposizione e le leggi nazionali che già disciplinano tale materia.

60. Innanzitutto, in merito all'articolo 4, paragrafo 1, della proposta, EDPB e GEPD sottolineano che l'articolo 9, paragrafo 1, GDPR, in linea di principio, non consente il trattamento di dati personali relativi alla salute e di dati genetici, fatto salvo il caso in cui si applichino le esenzioni di cui all'articolo 9, paragrafo 2, GDPR. Di conseguenza EDPB e GEPD raccomandano che l'articolo 4, paragrafo 1, della proposta sia allineato all'articolo 9, paragrafo 2, lettera h), GDPR.

61. In secondo luogo, EDPB e GEPD ritengono che tale disposizione non sia in linea con i principi del GDPR di minimizzazione dei dati e limitazione delle finalità, dato che l'accesso non è concesso soltanto laddove necessario e in base alla necessità di conoscere. Pertanto, anche al fine di fornire garanzie adeguate agli interessati, EDPB e GEPD raccomandano di introdurre che tale accesso avvenga soltanto in base alla necessità di conoscere.

62. In terzo luogo, EDPB e GEPD sottolineano che il concetto di "professionista sanitario" comprende una grande varietà di professioni di natura distinta e che richiedono tipi di coinvolgimento, processo decisionale e responsabilità diversi (ad esempio medici, infermieri, tecnici di laboratorio e di diagnostica per immagini, nutrizionisti, fisioterapisti, psicologi, tecnici farmaceutici). Di conseguenza EDPB e GEPD raccomandano che non tutti i dati sanitari siano resi disponibili a tutti i professionisti sanitari indiscriminatamente, ma soltanto a coloro rispetto ai quali tale accesso è ritenuto necessario ai fini dello svolgimento di un compito specifico. In questo contesto EDPB e GEPD sottolineano l'importanza dei principi di necessità e proporzionalità a questo riguardo. EDPB e GEPD rilevano che, ai sensi dell'articolo 4, paragrafo 2, della proposta, gli Stati membri, in linea con il principio di minimizzazione dei dati, devono stabilire norme che prevedano le categorie di dati sanitari elettronici personali necessarie per le diverse professioni sanitarie. EDPB e GEPD prendono atto che la proposta attribuisce esplicitamente tale responsabilità agli Stati membri, rendendola obbligatoria. A tal fine EDPB e GEPD raccomandano di sostituire la parola "possono" con "devono" affinché sia garantito che tali norme siano definite dagli Stati membri.

63. EDPB e GEPD rilevano che l'articolo 4, paragrafo 3, della proposta stabilisce che i professionisti sanitari abbiano accesso almeno alle categorie prioritarie di dati sanitari elettronici di cui all'articolo 5 della proposta, senza stabilire se tutti i professionisti sanitari debbano avere accesso a tutte le categorie prioritarie. Come indicato in precedenza, EDPB e GEPD ritengono che l'accesso dovrebbe essere concesso soltanto tenendo conto di quanto necessario ai fini delle cure sanitarie. Essi ritengono che nella proposta sia necessario chiarire ulteriormente il rapporto tra i paragrafi 2 e 3 dell'articolo 4 della proposta stessa.

64. L'articolo 4, paragrafo 4, della proposta prevede la possibilità di derogare alle limitazioni all'accesso selezionate dall'interessato, previste all'articolo 3, paragrafo 9, della proposta, qualora tale accesso sia necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica. Al riguardo EDPB e GEPD raccomandano ai colegislatori di specificare che il diritto delle persone fisiche di ottenere informazioni sull'accesso ai propri dati sanitari elettronici da parte dei professionisti sanitari previsto dall'articolo 3, paragrafo 10, comprende gli accessi alle informazioni soggette alle limitazioni di cui all'articolo 3, paragrafo 9, della proposta.

65. L'articolo 7 della proposta impone agli Stati membri di garantire che i professionisti sanitari registrino "sistematicamente" i dati sanitari pertinenti relativi ai servizi sanitari da essi prestati alle persone fisiche, in formato elettronico all'interno di un sistema di cartelle cliniche elettroniche. EDPB e GEPD esprimono preoccupazione in merito al riferimento a tale registrazione sistematica dato che sembra non essere in linea con il principio di minimizzazione dei dati di cui al GDPR. Di conseguenza suggeriscono di modificare il testo della proposta sopprimendo il termine "sistematicamente" al fine di allineare la disposizione al principio di minimizzazione dei dati.

66. EDPB e GEPD accolgono con favore le disposizioni sulla gestione dell'identità elettronica di cui all'articolo 9 della proposta poiché ritengono che l'identificazione e l'autenticazione sicure delle persone fisiche e dei professionisti sanitari che utilizzano servizi sanitari elettronici o accedono a dati sanitari personali siano uno degli aspetti fondamentali per tutelare i diritti degli interessati. A tale riguardo, EDPB e GEPD sottolineano che potrebbe essere necessario prevedere meccanismi diversi per l'identificazione e l'autenticazione per i professionisti sanitari a seconda che i loro accessi siano svolti in veste di professionisti o a titolo privato.

67. Per quanto concerne l'istituzione dell'autorità di sanità digitale, di cui all'articolo 10 della proposta, EDPB e GEPD esprimono preoccupazione in merito al fatto che taluni dei compiti di detta autorità

possano sovrapporsi a quelli delle autorità di controllo della protezione dei dati ai sensi del GDPR, in particolare in merito ai diritti dell'interessato e alla sicurezza del trattamento dei dati. Per motivi di certezza del diritto nonché per migliorare la leggibilità del testo giuridico, EDPB e GEPD suggeriscono di spostare la disposizione di cui all'articolo 3, paragrafo 11, ultima frase, della proposta all'articolo 10 della stessa.

68. In relazione all'articolo 11 della proposta, che sancisce il diritto per le persone fisiche e giuridiche di presentare un reclamo all'autorità di sanità digitale, EDPB e GEPD ritengono che il semplice fornire informazioni sull'esistenza della possibilità di un reclamo alle autorità di protezione dei dati non sia sufficiente per consentire loro di esaminare, indagare e valutare qualsiasi aspetto del reclamo per quanto concerne la protezione dei dati. Pertanto EDPB e GEPD raccomandano di chiarire che, se il reclamo ha in qualche modo una relazione con la protezione dei dati, anche se l'oggetto è connesso ai nuovi diritti spettanti alle persone fisiche introdotti dall'articolo 3 della proposta, l'autorità di sanità digitale deve trasmettere copia del reclamo all'autorità di controllo della protezione dei dati pertinente.

69. Più in generale, EDPB e GEPD suggeriscono di introdurre una consultazione obbligatoria e un obbligo di cooperazione con le autorità di protezione dei dati per quanto concerne la valutazione di reclami e l'attuazione della proposta ogniqualvolta siano coinvolti aspetti relativi alla protezione dei dati. Inoltre, EDPB e GEPD sottolineano che le autorità per la protezione dei dati sono le uniche autorità competenti responsabili per le questioni relative alla protezione dei dati e pertanto dovrebbero rimanere l'unico punto di contatto per l'interessato in merito a tali questioni, anche al fine di evitare qualsiasi confusione tra gli interessati circa le modalità con cui possono far valere i propri diritti alla protezione dei dati.

70. L'articolo 13 della proposta prevede la possibilità che tramite MyHealth@EU siano forniti servizi sanitari digitali transfrontalieri supplementari e che tale piattaforma sia in grado di scambiare dati con altre infrastrutture o altri servizi nei settori sanitario, dell'assistenza o della sicurezza sociale. La medesima disposizione impone agli Stati membri e alla Commissione di adoperarsi per garantire l'interoperabilità di MyHealth@EU con i sistemi tecnologici istituiti a livello internazionale per lo scambio di dati sanitari elettronici.

71. EDPB e GEPD rilevano che tali possibilità sono presentate in termini generali e che è piuttosto poco chiaro in quali circostanze e a quali condizioni i dati sanitari elettronici possono essere condivisi con partecipanti in paesi terzi. Alla luce delle garanzie richieste dal capo V GDPR per i trasferimenti internazionali di dati, EDPB e GEPD raccomandano ai colegislatori di chiarire che il controllo di conformità che deve essere svolto dalla Commissione per quanto concerne il punto di contatto nazionale del paese terzo o del sistema istituito a livello internazionale deve riguardare anche il soddisfacimento delle prescrizioni di cui al capo V GDPR, prima di stabilire tramite un atto di esecuzione che tale punto di contatto o sistema nazionale è conforme ai requisiti di MyHealth@EU ai fini dello scambio di dati sanitari elettronici.

6 SISTEMI DI CARTELLE CLINICHE ELETTRONICHE E APPLICAZIONI PER IL BENESSERE (CAPO III)

72. Il capo III della proposta si concentra sull'attuazione di uno schema di autocertificazione obbligatoria per i sistemi di cartelle cliniche elettroniche, nell'ambito del quale tali sistemi devono essere conformi alle prescrizioni essenziali relative all'interoperabilità e alla sicurezza di cui all'allegato II della

proposta. Come sottolineato nella relazione, "*[q]uesto approccio è necessario per garantire che le cartelle cliniche elettroniche siano compatibili con ciascun sistema e per facilitare la trasmissione dei dati sanitari elettronici tra loro*". EDPB e GEPD accolgono con favore il fatto che, ai sensi degli articoli 15 e 17 della proposta, i sistemi di cartelle cliniche elettroniche debbano essere soggetti a una procedura di valutazione della conformità preventiva prima che detti sistemi possano essere immessi sul mercato o altrimenti messi in servizio nell'UE.

73. Tuttavia EDPB e GEPD rilevano che talune delle prescrizioni essenziali di cui all'allegato II della proposta fanno riferimento ad aspetti relativi alla protezione dei dati personali, come quelli concernenti l'attuazione dei diritti delle persone fisiche, di cui al capo II della proposta, ossia relativi al trattamento sicuro dei dati sanitari elettronici[22]. Inoltre le specifiche comuni che la Commissione dovrà adottare, mediante atti di esecuzione, in relazione alle prescrizioni essenziali di cui all'allegato II, a norma dell'articolo 23, paragrafo 3, della proposta, possono riguardare aspetti relativi alla protezione dei dati, quali prescrizioni relative alla qualità dei dati, comprese la completezza e l'accuratezza dei dati sanitari elettronici, nonché prescrizioni e principi relativi alla sicurezza, alla riservatezza, all'integrità, alla sicurezza dei pazienti e alla protezione dei dati sanitari elettronici[23].

74. Innanzitutto EDPB e GEPD sottolineano che la conformità dei sistemi di cartelle cliniche elettroniche rispetto alle prescrizioni essenziali in materia di interoperabilità e sicurezza di cui all'allegato II della proposta non significa necessariamente che le operazioni di trattamento alla base del loro funzionamento siano di per sé lecite, dato che il titolare del trattamento potrebbe dover rispettare ulteriori prescrizioni risultanti dalla normativa UE in materia di protezione dei dati. Tuttavia sebbene EDPB e GEPD comprendano che le suddette prescrizioni essenziali e le specifiche comuni non siano direttamente collegate alla normativa UE in materia di protezione dei dati, alcune di esse possono avere ripercussioni significative sugli aspetti pertinenti per la protezione dei dati personali degli interessati coinvolti. A tale proposito EDPB e GEPD rilevano che le suddette prescrizioni non sembrano tenere debitamente conto dei principi di minimizzazione dei dati e di protezione dei dati fin dalla progettazione come aspetti chiave da tenere in considerazione nella progettazione di un sistema di cartelle cliniche elettroniche al fine di salvaguardare adeguatamente gli interessi e i diritti degli interessati in materia di protezione dei dati e tutela della vita privata. Inoltre le prescrizioni relative ai periodi di conservazione e ai diritti di accesso di cui al punto 3.8 dell'allegato II della proposta non tengono conto della finalità specifica delle operazioni di trattamento dei dati quale aspetto chiave da considerare per progettare le caratteristiche di conservazione di un sistema di cartelle cliniche elettroniche, oltre a tener conto "delle origini e delle categorie dei dati sanitari elettronici".

75. Considerando i rischi posti dalle disposizioni concernenti la disponibilità obbligatoria, la condivisione transfrontaliera, l'accesso e ulteriori usi dei dati sanitari elettronici contenuti nei sistemi di cartelle cliniche elettroniche così come l'impatto sulle persone interessate, EDPB e GEPD sono dell'opinione che, al fine di rafforzare la protezione delle persone e la loro fiducia in tali sistemi, sarebbe più adeguato introdurre una procedura di valutazione della conformità da parte di terzi per i sistemi di

[22] Cfr. ad esempio il punto 1.3 e le prescrizioni in materia di sicurezza di cui al punto 3 dell'allegato II, quali i punti 3.1. sulla prevenzione dell'accesso non autorizzato; 3.2. sui meccanismi per l'identificazione e l'autenticazione; 3.3. sui meccanismi di controllo dell'accesso; 3.4. sui meccanismi di registrazione per gli accessi ai dati; e 3.5. sui meccanismi di limitazione dell'accesso da parte dei professionisti sanitari.
[23] Cfr. articolo 23, paragrafo 3, lettere c) ed e), della proposta, nonché l'articolo 10, paragrafo 2, lettera h), della proposta.

cartelle cliniche elettroniche[24], coinvolgendo gli organismi notificati nella valutazione delle misure, comprese le soluzioni tecniche, adottate dal fabbricante per rispettare le prescrizioni in materia di interoperabilità e sicurezza di cui all'allegato II della proposta. A tale proposito, EDPB e GEPD rilevano positivamente che tale questione sarà oggetto di un esame specifico nel contesto della valutazione e del riesame della proposta effettuata dalla Commissione dopo 5 anni dalla sua entrata in vigore.

76. Inoltre EDPB e GEPD raccomandano di modificare la proposta in modo da chiarire la relazione tra lo schema di autocertificazione obbligatoria per i sistemi di cartelle cliniche elettroniche e le prescrizioni in materia di protezione dei dati. Occorre altresì sottolineare che, qualora le specifiche comuni di cui all'articolo 23 della proposta incidano sulle prescrizioni in materia di protezione dei dati per i sistemi di cartelle cliniche elettroniche, gli atti di esecuzione che devono essere adottati dalla Commissione a norma dell'articolo 23 della proposta dovrebbero essere oggetto di una consultazione tanto del GEPD quanto dell'EDPB conformemente all'articolo 42, paragrafo 2, EUDPR. Le medesime considerazioni valgono per l'etichettatura volontaria delle applicazioni per il benessere che si basano parimenti sulle prescrizioni essenziali di cui all'allegato II della proposta e sulle specifiche comuni di cui all'articolo 23 della stessa.

77. Per quanto concerne la gestione dei rischi posti dai sistemi di cartelle cliniche elettroniche e degli incidenti gravi, nonché l'attuazione di azioni correttive, ai sensi dell'articolo 29 della proposta, EDPB e GEPD raccomandano l'istituzione di un obbligo di informazione e cooperazione con le autorità di protezione dei dati, laddove pertinente. Non è infatti chiaro se il riferimento al rischio relativo ad "altri aspetti della protezione del pubblico interesse" tra i rischi che possono essere presentati da un sistema di cartelle cliniche elettroniche, che comporta quindi l'intervento dell'autorità di vigilanza del mercato, possa includere la protezione dei dati personali. Inoltre non si può escludere che un incidente grave che coinvolga un sistema di cartelle cliniche elettroniche [25] derivi da malfunzionamenti o deterioramenti delle caratteristiche o delle prestazioni di un tale sistema che incidono anche sulla protezione dei dati personali.

78. EDPB e GEPD in linea di principio accolgono con favore l'articolo 31 della proposta concernente l'etichettatura volontaria delle applicazioni per il benessere, dato che ciò può garantire trasparenza per gli utenti di tali applicazioni in merito alle loro caratteristiche principali, sostenendo così gli utenti nella scelta di applicazioni per il benessere affidabili. Tuttavia gli articoli 31 e 32 della proposta riguardano esclusivamente l'interoperabilità delle applicazioni per il benessere con i sistemi di cartelle cliniche elettroniche e istituiscono un meccanismo di conformità volontaria limitato alle prescrizioni in materia di interoperabilità e sicurezza di cui all'allegato II della proposta, al fine di garantire che le applicazioni per il benessere siano in grado di trasmettere dati sanitari elettronici a tali sistemi.

79. A tale proposito, EDPB e GEPD sottolineano che l'etichetta che accompagna le applicazioni per il benessere ai sensi dell'articolo 31 della proposta non significa necessariamente che le operazioni di trattamento alla base del funzionamento di tali applicazioni siano di per sé lecite e possano essere utilizzate dall'utente in quanto tali. Il titolare del trattamento dovrà rispettare ulteriori prescrizioni derivanti dalla normativa UE in materia di protezione dei dati. EDPB e EDPB raccomandano di chiarire tale aspetto nella proposta, anche in un considerando. Il considerando 35 della proposta afferma che

[24] Cfr. ad esempio la procedura di valutazione della conformità da parte di terzi di cui al regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio.
[25] Cfr. definizione di cui all'articolo 2, paragrafo 2, lettera q), della proposta.

"*[g]li utenti di applicazioni per il benessere, quali le applicazioni mobili, dovrebbero essere informati sulla capacità di tali applicazioni di essere collegate e di fornire dati ai sistemi di cartelle cliniche elettroniche o a soluzioni di sanità elettronica nazionali, nei casi in cui i dati prodotti dalle applicazioni per il benessere siano utili per finalità di assistenza sanitaria*". Tuttavia le condizioni alle quali tali applicazioni per il benessere possono essere lecitamente collegate e fornire dati personali ai sistemi di cartelle cliniche elettroniche (o alle soluzioni di sanità elettronica nazionali) ai sensi della legislazione in materia di protezione dei dati non sono specificate nella proposta. Ciò che appare evidente dall'elenco delle categorie minime di dati elettronici per l'uso secondario, di cui all'articolo 33 della proposta, è che indirettamente, una volta caricati in un sistema di cartelle cliniche elettroniche[26], o direttamente, nella misura in cui vengano raccolti e/o trattati da soggetti che rientrano nella definizione di titolari dei dati di ai sensi dell'articolo 2, paragrafo 2, lettera y), della proposta[27], i dati personali prodotti dalle applicazioni per il benessere rientrano in tali categorie e sono quindi soggetti all'obbligo per i titolari dei dati di renderli disponibili per un uso secondario conformemente alle disposizioni di cui al capo IV della proposta.

80. La disponibilità obbligatoria di dati sanitari elettronici generati da dispositivi medici, applicazioni per il benessere o altre applicazioni di sanità digitale per l'uso secondario deve essere valutata alla luce dei rapidi sviluppi tecnologici nel contesto della tecnologia mobile e indossabile e della crescente popolarità di applicazioni mobili e dispositivi di "auto quantificazione", che consentono alle persone di registrare tutti i tipi di aspetti concernenti la loro personalità, la loro mente, il loro corpo, i loro modelli comportamentali e i loro spostamenti. Chiaramente queste tipologie di trattamento dei dati meritano una notevole attenzione, in quanto non è facile per gli interessati riconoscerle come trattamento di dati sanitari. Tuttavia ciò comporta nel contempo rischi effettivi per la tutela della vita privata, soprattutto nel caso in cui tali dati siano trattati per finalità supplementari e/o combinati con altri dati o ceduti a terzi. Questi tipi di trattamento dei dati possono creare rischi specifici, compreso quello di un trattamento iniquo o ingiusto basato su dati concernenti lo stato di salute presunto o effettivo di una persona derivati, ad esempio attraverso la profilazione, da dettagli molto intimi riguardanti la sua vita privata, indipendentemente dal fatto che tali conclusioni sul suo stato di salute siano esatte o meno. In effetti tali rischi possono essere collegati altresì all'affidabilità e all'accuratezza dei dati generati da dispositivi medici, applicazioni per il benessere o altre applicazioni di sanità digitale. In tale contesto EDPB e GEPD riconoscono che l'articolo 33, paragrafo 3, tenta di delimitare quali dati generati da dispositivi medici, applicazioni per il benessere o altre applicazioni di sanità digitale debbano essere resi disponibili per usi secondari. Tuttavia EDPB e GEPD sottolineano che non è comunque chiaro quale tipo di dati rientri in tale categoria o chi ne valuterebbe la validità e la qualità una volta inseriti dalle persone nella propria cartella clinica elettronica ai sensi dell'articolo 3, paragrafo 6, e dell'articolo 33, paragrafo 1, lettera a), della proposta oppure resi direttamente disponibili dai titolari dei dati ai sensi dell'articolo 33, paragrafo 1, lettere f) ed n), della proposta.

81. A questo proposito EDPB e GEPD raccomandano di escludere dall'ambito di applicazione del capo IV della proposta le applicazioni per il benessere e altre applicazioni digitali. Qualora tali dati dovessero essere mantenuti nell'ambito di applicazione del capo IV, EDPB e GEPD sottolineano che gli utenti devono rimanere liberi di decidere se e quali dei propri dati personali generati dall'applicazione per il benessere e da altre applicazioni digitali, indipendentemente dal fatto che siano stati caricati nelle proprie cartelle cliniche elettroniche, debbano essere condivisi con altri destinatari e trattati

[26] Cfr. articolo 3, paragrafo 6, e articolo 33, paragrafo 1, lettera a), della proposta.
[27] Cfr. articolo 33, paragrafo 1, lettere f) ed n), della proposta.

ulteriormente per usi secondari. Pertanto EDPB e GEPD raccomandano di modificare la proposta in modo da garantire che gli interessati siano adeguatamente informati in merito alle scelte a loro disposizione per quanto concerne i potenziali ulteriori usi dei loro dati sanitari elettronici, compresi quelli generati da applicazioni per il benessere e altre applicazioni digitali. In secondo luogo, occorre stabilire in modo chiaro le condizioni specifiche per l'ulteriore trattamento di tali dati personali in conformità con la normativa in materia di protezione dei dati; occorre altresì stabilire meccanismi adeguati per garantire il rispetto delle volontà degli interessati in merito all'ulteriore trattamento dei loro dati sanitari personali generati da applicazioni per il benessere e altre applicazioni digitali.

7 USO SECONDARIO DEI DATI SANITARI ELETTRONICI (CAPO IV)

82. EDPB e GEPD riconoscono che il capo IV della proposta mira a facilitare l'uso secondario dei dati sanitari elettronici e accolgono con favore il fatto che tale uso possa generare notevoli vantaggi per il bene pubblico. Tuttavia EDPB e GEPD ritengono che tali ulteriori attività di trattamento non siano prive di rischi per i diritti e le libertà degli interessati.

83. EDPB e GEPD prendono atto del fatto che, in linea con il considerando 37 della proposta, il "*[...] regolamento fornisce la base giuridica in conformità dell'articolo 9, paragrafo 2, lettere g), h), [...] e j), del regolamento (UE) 2016/679 per l'uso secondario dei dati sanitari, stabilendo le garanzie per il trattamento, in termini di finalità legittime, una governance affidabile per fornire l'accesso ai dati sanitari (attraverso organismi responsabili dell'accesso ai dati sanitari) e il trattamento in un ambiente sicuro, nonché modalità per il trattamento dei dati, stabilite nell'autorizzazione ai dati*". In tale contesto, il medesimo considerando prevede che il richiedente dimostrerà una base giuridica ai sensi dell'articolo 6 GDPR, sulla base della quale potrebbe essere presentata una richiesta di accesso ai dati alla luce della proposta, mentre ciò non trova necessariamente riscontro nel dispositivo della proposta. Al contrario, EDPB e GEPD rilevano che l'articolo 34, paragrafo 1, della proposta fornisce un elenco di finalità per le quali i dati sanitari elettronici possono essere trattati per un uso secondario, che comprendono, a titolo esemplificativo ma non esaustivo, la finalità delle attività di ricerca scientifica nel settore sanitario o dell'assistenza.

84. A tale proposito, EDPB e GEPD hanno avanzato tre preoccupazioni principali.

85. **Innanzitutto** EDPB e GEPD rilevano una mancanza di un'adeguata definizione delle finalità elencate all'articolo 34, paragrafo 1, della proposta per le quali i dati sanitari elettronici possono essere ulteriormente trattati, e in particolare esprimono preoccupazione per quanto concerne l'articolo 34, paragrafo 1, lettere f) e g), della proposta, che possono comprendere qualsiasi forma di "attività di sviluppo e innovazione per prodotti o servizi che contribuiscono alla sanità pubblica o alla sicurezza sociale" o "attività di addestramento, prova e valutazione degli algoritmi, anche nell'ambito di dispositivi medici, sistemi di IA e applicazioni di sanità digitale, che contribuiscono alla sanità pubblica o alla sicurezza sociale". EDPB e GEPD raccomandano vivamente che la proposta definisca ulteriormente tali finalità e circoscriva quando vi è un collegamento sufficiente con la sanità pubblica e/o la sicurezza sociale, al fine di raggiungere un equilibrio che tenga adeguatamente conto degli obiettivi perseguiti dalla proposta e della protezione dei dati personali degli interessati coinvolti nel trattamento.

86. **In secondo luogo**, alla luce delle osservazioni di cui sopra e nonostante la formulazione contenuta al considerando 37 della proposta, EDPB e GEPD ritengono che la proposta richieda ulteriori miglioramenti per garantire il rispetto dell'articolo 9 GDPR.

87. In effetti le finalità per le quali è possibile trattare dati sanitari elettronici per l'uso secondario ai sensi dell'articolo 34, paragrafo 1, della proposta contempla tipi diversi di uso secondario, che rientrerebbero in categorie diverse di motivi di eccezione previsti dall'articolo 9, paragrafo 2, GDPR. Tuttavia EDPB e GEPD ritengono che ciò non si rispecchi nei criteri in base ai quali gli organismi responsabili dell'accesso ai dati sanitari dovrebbero valutare e decidere in merito alle domande di accesso ai dati (articolo 45 della proposta) al fine di rilasciare un'autorizzazione di accesso ai dati (articolo 46 della proposta). A tal fine EDPB e GEPD sottolineano che i criteri previsti al riguardo dall'articolo 46 della proposta sono limitati alle disposizioni e ai principi della proposta stessa e mancano di chiarezza circa il modo in cui tali disposizioni si riferiscono ai principi e alle disposizioni di cui al GDPR, in particolare all'articolo 9, paragrafo 2, GDPR.

88. In aggiunta a quanto sopra, EDPB e GEPD chiedono chiarimenti specifici circa le modalità e i casi in cui l'articolo 9, paragrafo 2, lettera j), GDPR sarebbe applicabile nei casi di trattamento di dati sanitari "a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici" (ai sensi del diritto dell'Unione o di quello degli Stati membri) e in relazione a "garanzie adeguate" come richiesto dall'articolo 89, paragrafo 1, GDPR.

89. **In terzo luogo**, EDPB e GEPD si chiedono come tale eccezione, interpretata ai sensi del diritto dell'Unione, rispetto all'articolo 9, paragrafo 2, GDPR, possa essere conciliata con l'articolo 9, paragrafo 4, GDPR e la possibilità concessa al diritto degli Stati membri di introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute. A tale riguardo, EDPB e GEPD ritengono che la proposta potrebbe chiarire come l'eccezione rispetto all'articolo 9, paragrafo 1, GDPR, derivante dalla proposta ma ad ora non ancora esplicitamente specificata in nessuna delle disposizioni della proposta, intenda conciliarsi con tutte le legislazioni nazionali dei diversi Stati membri.

90. Di conseguenza**, EDPB e GEPD chiedono che la proposta assicuri la piena compatibilità con l'articolo 9, paragrafo 2, GDPR e in particolare per quanto riguarda la sua applicazione alle finalità di cui all'articolo 34, paragrafo 1, lettere f) e g), della proposta**. Inoltre EDPB e GEPD raccomandano altresì di modificare di conseguenza l'articolo 46 della proposta, al fine di integrare e rispecchiare adeguatamente le differenze negli obiettivi e nelle prescrizioni previsti per l'uso secondario dei dati sanitari elettronici.

91. Per quanto concerne le **categorie minime di dati elettronici per l'uso secondario**, EDPB e GEPD rilevano che, ai sensi dell'articolo 33, paragrafo 1, della proposta, si interpreta un obbligo giuridico, secondo il quale i titolari dei dati, mediante il diritto dell'Unione, devono mettere a disposizione categorie specifiche di dati sanitari elettronici per l'uso secondario. EDPB e GEPD osservano che l'articolo 41, paragrafo 1, della proposta indica che tale (nuovo) obbligo giuridico integra qualsiasi altro obbligo giuridico (già) previsto in altri atti del diritto dell'Unione o della normativa nazionale di attuazione del diritto dell'Unione. Come indicato nel considerando 37 della proposta, EDPB e GEPD rilevano che l'articolo 33, paragrafo 1, della proposta fungerebbe da fondamento giuridico ai sensi dell'articolo 6, paragrafo 1, lettera c), GDPR e prevedrebbe altresì un'eccezione al divieto di cui all'articolo 9, paragrafo 1, GDPR per il trattamento (quindi la messa a disposizione e la fornitura) dei dati sanitari elettronici personali da parte del titolare dei dati. A questo proposito, sebbene EDPB e GEPD riconoscano che tale obbligo giuridico per i titolari dei dati, in linea di principio, si inserisce nel sistema del GDPR, esso può comportare incertezza del diritto.

92. A tale riguardo, l'articolo 33, paragrafo 5, della proposta lo prevede che "*[q]ualora il diritto nazionale prescriva il consenso della persona fisica, gli organismi responsabili dell'accesso ai dati sanitari si*

basano sugli obblighi di cui al presente capo per fornire l'accesso ai dati sanitari elettronici". EDPB e GEPD ritengono innanzitutto che non sia chiaro il tipo di "prescrizioni in materia di consenso" previste dal diritto nazionale a cui la disposizione fa riferimento. In particolare **EDPB e GEPD sottolineano la mancanza di chiarezza in merito alla fase della procedura prevista nella proposta per quanto riguarda l'uso secondario dei dati sanitari elettronici nella quale gli organismi responsabili dell'accesso ai dati sanitari possono ignorare tali prescrizioni stabilite nel diritto nazionale**, in particolare quando ciò rientra nell'ambito di applicazione dell'articolo 9, paragrafo 4, GDPR. EDPB e GEPD raccomandano altresì di fornire ulteriori chiarimenti e precisazioni in relazione all'articolo 46, paragrafo 6, lettera f), della proposta, il quale prevede che l'organismo responsabile dell'accesso ai dati sanitari introduca eventualmente "condizioni specifiche [...] stabilite nell'autorizzazione ai dati concessa".

93. L'articolo 36 della proposta prevede **l'istituzione di organismi responsabili dell'accesso ai dati sanitari**. A tale proposito, EDPB e GEPD sottolineano che la competenza dell'organismo responsabile dell'accesso ai dati sanitari per la valutazione della base giuridica proposta dall'utente dei dati richiederà la disponibilità di un'adeguata competenza giuridica in seno a detto organismo. EDPB e GEPD osservano che, per il momento, ciò non è espressamente indicato all'articolo 36 della proposta. Tuttavia EDPB e GEPD sottolineano che la valutazione della base giuridica da parte dell'organismo responsabile dell'accesso ai dati sanitari può, sempre, essere esaminata e, ove necessario, ribaltata dall'autorità di protezione dei dati pertinente. A tal fine, EDPB e GEPD chiedono chiarezza specifica in merito all'interazione tra il ruolo dell'organismo responsabile dell'accesso ai dati sanitari e la rispettiva autorità di protezione dei dati nel contesto di qualsiasi questione connessa alla protezione dei dati.

94. La necessità di chiarire il rapporto tra la proposta e la normativa degli Stati membri è ulteriormente esemplificata nel contesto delle **domande di autorizzazioni ai dati nel contesto dell'accesso transfrontaliero ai dati sanitari elettronici personali per l'uso secondario** (sezione 4, articoli da 52 a 54 della proposta). EDPB e GEPD osservano che, sebbene la proposta miri a facilitare l'uso secondario transfrontaliero, istituendo "punti di contatto nazionali" e un'infrastruttura transfrontaliera (HealthData@EU), gli utenti dei dati dovranno probabilmente comunque presentare domanda ai rispettivi organismi responsabili dell'accesso ai dati sanitari in ciascuno degli Stati membri. In effetti, secondo l'interpretazione di EDPB e GEPD l'articolo 45, paragrafo 3, della proposta prevede soltanto un coordinamento limitato tra gli organismi responsabili dell'accesso ai dati sanitari coinvolti, ai fini dell'ottenimento di un'autorizzazione ai dati. Tuttavia EDPB e GEPD ritengono che la proposta non offra chiarimenti adeguati in merito alla specifica normativa nazionale che sarà applicata nel contesto delle autorizzazioni transfrontaliere ai dati (quella del rispettivo organismo responsabile dell'accesso ai dati sanitari o quella del richiedente), compresa la base giuridica che dovrà essere individuata (da parte del richiedente) e valutata (dall'organismo responsabile dell'accesso ai dati sanitari). Si segnala infine, a tale proposito, che tanto dalla parte dell'organismo responsabile dell'accesso ai dati sanitari, quanto dalla parte dell'utente dei dati possono sussistere carenze (significative) in termini di competenze per superare problemi di individuazione e valutazione delle differenze presenti tra le (prescrizioni da soddisfare come previsto dalle) normative degli Stati membri concernenti una (tale) base giuridica.

95. EDPB e GEPD osservano che l'articolo 38, paragrafo 2, della proposta stabilisce che gli organismi responsabili dell'accesso ai dati sanitari non sono tenuti a fornire le informazioni specifiche di cui all'articolo 14 GDPR a ciascuna persona fisica in merito all'uso dei suoi dati per progetti sottoposti a un'autorizzazione ai dati. A tale proposito, EDPB e GEPD ritengono che l'esenzione introdotta possa

comportare conseguenze indesiderate per i diritti e le libertà fondamentali degli interessati, in ragione della mancanza di condizioni concrete alle quali tale esenzione sarebbe applicabile.

96. EDPB e GEPD ricordano inoltre l'importanza degli obblighi di trasparenza nei confronti degli interessati e sollecitano il colegislatore a individuare situazioni specifiche per garantire che tale disposizione non possa essere invocata sistematicamente dagli organismi responsabili dell'accesso ai dati sanitari. Pertanto EDPB e GEPD raccomandano di modificare la disposizione di conseguenza tenendo conto del fatto che le prescrizioni di cui all'articolo 14 del GDPR non possono essere eluse sistematicamente senza una valutazione e una giustificazione adeguate e pertinenti della necessità di fare affidamento su tale esenzione[28]. Qualora sia mantenuta la limitazione del diritto all'informazione, EDPB e GEPD evidenziano ai colegislatori la necessità di considerare le condizioni previste dall'articolo 23 GDPR.

97. L'articolo 40 della proposta definisce e prevede l'altruismo dei dati nel settore sanitario. Al riguardo EDPB e GEPD considerano tale disposizione poco chiara, in particolare per quanto concerne la sua interazione con la rispettiva disposizione introdotta dall'atto sulla governance dei dati. A tal fine EDPB e GEPD raccomandano di chiarire la disposizione di conseguenza.

98. EDPB e GEPD prendono atto positivamente della disposizione di cui all'articolo 44, paragrafo 3, della proposta, ai sensi della quale, laddove gli organismi responsabili dell'accesso ai dati sanitari debbano fornire accesso ai dati in formato pseudonimizzato, gli utenti dei dati non devono reidentificare i dati sanitari elettronici forniti in tale formato (le informazioni per invertire la pseudonimizzazione devono essere disponibili soltanto per gli organismi responsabili dell'accesso ai dati sanitari). EDPB e GEPD accolgono inoltre con favore il fatto che la stessa disposizione della proposta stabilisca che in caso di mancato rispetto da parte dell'utente dei dati delle misure dell'organismo responsabile dell'accesso ai dati sanitari utilizzate per garantire la pseudonimizzazione, il primo è soggetto a sanzioni adeguate.

99. Infine l'articolo 48 della proposta stabilisce che, in deroga all'articolo 46 della proposta stessa, per accedere ai dati sanitari elettronici di cui allo stesso articolo non è necessaria l'autorizzazione ai dati da parte di enti del settore pubblico e di istituzioni, organi e organismi dell'Unione. EDPB e GEPD ritengono che dovrebbe essere necessaria un'autorizzazione anche in tal caso, al fine di consentire la verifica del rispetto di tutte le prescrizioni pertinenti, comprese la liceità e la necessità. Inoltre EDPB e GEPD considerano tale prescrizione importante per promuovere la trasparenza, dato che la proposta prevede che gli organismi responsabili dell'accesso ai dati sanitari forniscano al pubblico informazioni su tutte le autorizzazioni ai dati rilasciate a norma dell'articolo 46.

8 ALTRE AZIONI (CAPO V)

8.1 Conservazione dei dati sanitari elettronici personali nell'UE e conformità dei trasferimenti internazionali di dati rispetto al capo V GDPR

100. Il capo V della proposta mira a suggerire altre misure che promuovano lo sviluppo delle capacità da parte degli Stati membri per sostenere la messa a punto dello spazio europeo dei dati sanitari. Inoltre tale capo disciplina l'accesso ai dati (sanitari) elettronici *non personali* e il trasferimento degli stessi a livello internazionale, così come l'accesso ai dati sanitari elettronici *personali* e il trasferimento degli stessi a livello internazionale.

[28] Cfr. anche il punto 25.

101. Per quanto concerne l'accesso ai dati sanitari elettronici *personali* e il trasferimento degli stessi a livello internazionale, l'articolo 63 della proposta specifica che gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, conformemente e alle condizioni di cui all'articolo 9, paragrafo 4, del regolamento (UE) 2016/679.

102. **Innanzitutto** EDPB e GEPD desiderano ricordare che, nella sua sentenza *Digital Rights Ireland*, la Corte ha ritenuto che l'assenza di un obbligo di conservazione dei dati all'interno dell'UE significava che "*[...] non si può ritenere pienamente garantito il controllo da parte di un'autorità indipendente, esplicitamente richiesto dall'articolo 8, paragrafo 3, della Carta, del rispetto dei requisiti di protezione e di sicurezza [...]. Orbene, siffatto controllo, effettuato in base al diritto dell'Unione, costituisce un elemento essenziale del rispetto della tutela delle persone riguardo al trattamento dei dati personali*"[29]. In altre parole, la Corte ha affermato espressamente, nel caso in questione, che il controllo del rispetto dei requisiti di protezione e di sicurezza da parte di un'autorità di controllo indipendente non può essere pienamente garantito in assenza dell'obbligo di conservare i dati in questione all'interno dell'UE. La mancata imposizione dell'obbligo di conservazione dei dati nell'UE rientrava tra le considerazioni che hanno portato la Corte a concludere che il legislatore dell'Unione aveva ecceduto i limiti imposti dal rispetto del principio di proporzionalità alla luce degli articoli 7, 8 e 52, paragrafo 1, della Carta[30].

103. La necessità di imporre un obbligo di conservazione dei dati personali nell'UE in alcuni casi specifici è stata quindi confermata e integrata nella sentenza *Tele 2* nella quale la Corte ha ritenuto che *"[t]enuto conto della quantità di dati conservati, del carattere sensibile dei dati stessi, nonché del rischio di accesso illecito a questi ultimi, i fornitori di servizi di comunicazione elettronica devono, al fine di assicurare la piena integrità e la riservatezza dei dati suddetti, garantire un livello particolarmente elevato di protezione e di sicurezza mediante misure tecniche e organizzative appropriate. In particolare, la normativa nazionale deve prevedere la conservazione nel territorio dell'Unione nonché la distruzione irreversibile dei dati al termine della durata di conservazione degli stessi"* (sottolineatura aggiunta)[31]. Ancora una volta la Corte ha sottolineato che per garantire il livello necessario di sicurezza e protezione dei dati in questione, la legislazione pertinente **deve** imporre che i dati siano conservati nell'UE.

104. EDPB e GEPD ritengono che le conclusioni cui è giunta la Corte in tali due sentenze di riferimento siano rilevanti anche nel contesto della proposta, in quanto si applicheranno i) al trattamento di una notevole quantità di dati personali, ii) che hanno natura altamente sensibile e iii) per i quali non esiste

---

[29] Sentenza della Corte di giustizia dell'8 aprile 2014, *Digital Rights Ireland Ltd*, cause riunite C-293/12 e C-594/12, ECLI:EU:C:2014:238, punto 68. Cfr. anche conclusioni dell'avvocato generale Cruz Villalón del 12 dicembre 2013 nel contesto della medesima causa, ai punti 78 e 79, ai quali si constata che l'assenza di una disposizione che stabilisca l'obbligo di "conservare [i dati] nel territorio di uno Stato membro, rientrante nella giurisdizione di uno Stato membro", "aggrava [...] il rischio di un uso non conforme agli obblighi derivanti dal diritto al rispetto della vita privata" e "aggrava considerevolmente il rischio che tali dati possano essere accessibili o divulgati in violazione di tale normativa".

[30] Sentenza della Corte di giustizia dell'8 aprile 2014, *Digital Rights Ireland Ltd*, cause riunite C-293/12 e C-594/12, ECLI:EU:C:2014:238, punto 69.

[31] Sentenza della Corte di giustizia del 21 dicembre 2016, *Tele2 Sverige AB/Post- och telestyrelsen e Secretary of State for the Home Department/Tom Watson e a.*, cause riunite C-203/15 e C-698/15, ECLI:EU:C:2016:970, punto 122. Cfr. anche conclusioni dell'avvocato generale H. Saugmandsgaard Øe, presentate il 19 luglio 2016, nella causa *Tele2 Sverige AB/Post- och telestyrelsen e Secretary of State for the Home Department/Tom Watson e a.*, cause riunite C-203/15 e C-698/15, punti da 239 a 241.

un elemento oggettivo che porti a concludere che il rischio di accesso illecito è inferiore a quello individuato nel contesto delle sentenze di cui sopra[32]. In particolare EDPB e GEPD sottolineano che è persino più probabile che la conclusione della Corte si applichi ai dati nel caso di specie considerando che è probabile che i dati sanitari siano considerati persino più sensibili dei dati relativi alle telecomunicazioni (ossia dei dati in questione nelle due sentenze di cui sopra).

105. In questo contesto, EDPB e GEPD condividono le preoccupazioni della Corte in merito alla necessità di attenuare i rischi di accesso illecito e di un controllo inefficace quando si tratta di determinati tipi di dati e taluni tipi di operazioni di trattamento. In particolare EDPB e GEPD osservano che nel caso in cui l'infrastruttura di trattamento si trovi in Stati non membri dell'UE/del SEE, il controllo da parte dell'autorità di controllo della protezione dei dati dell'UE sulla conformità rispetto alle norme UE in materia di protezione dei dati potrebbe non essere sempre pienamente garantito.

106. Inoltre EDPB e GEPD osservano che la Commissione ha recentemente proposto prescrizioni in materia di conservazione dei dati in un altro contesto: l'articolo 17, paragrafo 1, lettera c), della recente proposta di regolamento del Parlamento europeo e del Consiglio sulla sicurezza delle informazioni nelle istituzioni, negli organi e negli organismi dell'Unione prevede in effetti che "le informazioni sensibili non classificate dovrebbero essere conservate e trattate nell'Unione"[33]. Più in generale, EDPB e GEPD rilevano che il diritto dell'Unione fornisce già diversi esempi di atti legislativi esistenti che impongono la conservazione di dati personali nell'UE e che di solito vanno persino oltre, limitando anche i trasferimenti[34]. EDPB e GEPD concludono quindi che il diritto dell'Unione prevede, in alcune situazioni specifiche, di imporre che i dati siano conservati nell'UE al fine di attenuare il rischio di accesso illecito e di garantire un controllo efficace.

107. **In secondo luogo,** EDPB e GEPD osservano che l'articolo 62 della proposta, sull'accesso ai dati sanitari elettronici non personali e trasferimento degli stessi a livello internazionale, fa riferimento in diversi casi a dati sanitari elettronici non personali "detenuti nell'Unione", una circostanza questa che parrebbe indicare un presupposto generale secondo il quale tale categoria di dati dovrebbe essere conservata nell'UE. GEPD ed EDPB ritengono che il medesimo approccio dovrebbe essere adottato per

---

[32] EDPB e GEPD osservano che tale rischio di accesso illecito è tale da aver effettivamente condotto la Commissione a dedicare una disposizione specifica alla questione per ciò che riguarda i dati non personali (articolo 62 della proposta).

[33] Proposta di regolamento del Parlamento europeo e del Consiglio sulla sicurezza delle informazioni nelle istituzioni, negli organi e negli organismi dell'Unione (COM(2022) 119 final); https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A52022PC0119.

[34] Cfr. ad esempio articolo 6, paragrafo 8, della direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi (GU L 119 del 4.5.2016, pag. 132): "la conservazione, il trattamento e l'analisi dei dati PNR da parte dell'UIP sono effettuati esclusivamente in un luogo o in luoghi sicuri all'interno del territorio degli Stati membri"; articolo 3 del regolamento (CE) n. 767/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (regolamento VIS) (GU L 218 del 13.8.2008, pag. 60); articolo 41 del regolamento (UE) 2017/2226 del Parlamento europeo e del Consiglio, del 30 novembre 2017, che istituisce un sistema di ingressi/uscite per la registrazione dei dati di ingresso e di uscita e dei dati relativi al respingimento dei cittadini di paesi terzi che attraversano le frontiere esterne degli Stati membri e che determina le condizioni di accesso al sistema di ingressi/uscite a fini di contrasto e che modifica la Convenzione di applicazione dell'Accordo di Schengen e i regolamenti (CE) n. 767/2008 e (UE) n. 1077/2011 (GU L 327 del 9.12.2017, pag. 20); articolo 39 del regolamento (CE) n. 1987/2006 del Parlamento europeo e del Consiglio, del 20 dicembre 2006, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II) (GU L 381 del 28.12.2006, pag. 4).

i dati personali che rientrano nell'ambito di applicazione della proposta, in quanto sembrerebbe difficile giustificare l'esistenza di una prescrizione che impone la conservazione di dati sanitari elettronici non personali nell'UE ma l'assenza della medesima prescrizione per dati sanitari elettronici personali.

108. **In terzo luogo,** EDPB e GEPD desiderano chiarire in tale contesto che l'obbligo di conservare i dati personali nell'UE non preclude i trasferimenti di dati sanitari elettronici personali verso paesi terzi od organizzazioni internazionali. In effetti è possibile conciliare una prescrizione generale che prevede la conservazione di dati personali nell'UE con trasferimenti specifici considerati conformi al capo V GDPR (ad esempio nel contesto della ricerca scientifica, dell'erogazione di assistenza, della cooperazione internazionale). Di conseguenza EDPB e GEPD ritengono che l'obbligo di conservare i dati nell'UE sarebbe proporzionato e non andrebbe oltre quanto necessario per conseguire l'obiettivo perseguito, ossia quello di stabilire una garanzia supplementare al fine di attenuare il rischio di accesso illecito e controllo inefficace sui dati interessati, data la loro natura altamente sensibile.

109. **In quarto luogo,** EDPB e GEPD rilevano altresì che l'articolo 63 della proposta prevede che gli Stati membri possano mantenere o introdurre ulteriori condizioni, comprese limitazioni, conformemente e alle condizioni di cui all'articolo 9, paragrafo 4, GDPR. Tali limitazioni imposte a livello nazionale possono comprendere l'obbligo di conservare i dati nell'UE. EDPB e GEPD attirano l'attenzione sul fatto che tale obbligo si applica già in diversi Stati membri e considerano probabile che diversi Stati membri impongano o continuino a imporre obblighi analoghi qualora la questione non venga armonizzata a livello UE.

110. Alla luce di quanto sopra, EDPB e GEPD ritengono pertanto che sia essenziale evitare un approccio incoerente e frammentato nel territorio dell'UE che determinerebbe livelli diversi di protezione degli interessati, una circostanza questa che sarebbe in contrasto con uno degli obiettivi chiave del GDPR[35]. Di conseguenza EDPB e GEPD ritengono che obblighi supplementari, compresa la conservazione di dati sanitari elettronici personali all'interno dell'UE, dovrebbero essere affrontati nella massima misura possibile a livello di UE, ossia nella proposta, al fine di garantire un livello uniforme di protezione agli interessati in tutta l'Unione, nonché di preservare il corretto funzionamento del mercato interno, in linea con l'articolo 114 TFUE su cui si basa la proposta.

111. Per tutte le ragioni di cui sopra e tenendo conto della natura altamente sensibile dei dati personali in questione, **EDPB e GEPD ritengono che l'articolo 63 della proposta dovrebbe imporre ai titolari del trattamento e ai responsabili del trattamento stabiliti nell'UE che trattano dati sanitari elettronici personali soggetti all'ambito di applicazione della proposta l'obbligo di conservare tali dati nell'UE.** Come spiegato in precedenza, tale prescrizione che prevede la conservazione dei dati sanitari elettronici personali nell'UE **non** dovrebbe **pregiudicare la possibilità di trasferire i dati sanitari elettronici personali conformemente al capo V GDPR**[36]. EDPB e GEPD raccomandano altresì di ricordare nel preambolo che i titolari del trattamento e i responsabili del trattamento che trattano

[35] Cfr. considerando 53 GDPR relativo all'articolo 9, paragrafo 4, GDPR: "senza tuttavia ostacolare la libera circolazione dei dati personali all'interno dell'Unione quando tali condizioni si applicano al trattamento transfrontaliero degli stessi".
[36] E a patto che siano rispettate le altre condizioni del GDPR, in particolare l'articolo 6 GDPR concernente l'obbligo di liceità del trattamento.

dati sanitari elettronici personali rimangono soggetti all'applicazione dell'articolo 48 GDPR in materia di trasferimenti o comunicazioni non autorizzati dal diritto dell'Unione e devono rispettare tale disposizione in caso di richiesta di accesso derivante da un paese terzo[37].

8.2 Appalti pubblici e finanziamento dell'Unione

112. EDPB e GEPD rilevano che l'articolo 60 della proposta affronta la questione delle prescrizioni aggiuntive in materia di appalti pubblici e finanziamento dell'Unione. EDPB e GEPD ritengono che le raccomandazioni di cui sopra (in materia di conservazione dei dati nell'UE e rispetto del capo 5 e in particolare dell'articolo 48 GDPR) sarebbero rese operative nel migliore dei modi qualora fossero integrate in una fase iniziale delle procedure di appalto pubblico[38] e finanziamento di servizi forniti da titolari del trattamento e responsabili del trattamento stabiliti nell'UE che trattano dati sanitari elettronici personali.

113. Di conseguenza **EDPB e GEPD raccomandano che l'articolo 60 della proposta preveda anch'esso, come condizione per l'appalto o il finanziamento di servizi forniti da titolari del trattamento e responsabili del trattamento stabiliti nell'UE che trattano dati sanitari elettronici personali, che tali soggetti: i) conservino tali dati nell'UE; e ii) abbiano debitamente dimostrato di non essere soggetti a legislazioni di paesi terzi in conflitto con le norme dell'UE in materia di protezione dei dati.**

8.3 Punti di contatto nazionali di un paese terzo o sistemi istituiti a livello internazionale

114. EDPB e GEPD osservano che l'articolo 13, paragrafo 3 e l'articolo 52, paragrafo 5, della proposta prevedono la possibilità che i punti di contatto nazionali di un paese terzo o sistemi istituiti a livello internazionale siano riconosciuti conformi ai requisiti rispettivamente di MyHealth@EU e HealthData@EU. EDPB e GEPD ricordano che i trasferimenti derivanti dalla connessione e dall'uso di MyHealth@EU e HealthData@EU dovrebbero rispettare il capo V GDPR.

115. EDPB e GEPD osservano che l'articolo 13, paragrafo 3 e l'articolo 52, paragrafo 5, della proposta prevedono la possibilità che i punti di contatto nazionali di un paese terzo o sistemi istituiti a livello internazionale siano riconosciuti conformi ai requisiti rispettivamente di MyHealth@EU e HealthData@EU. EDPB e GEPD ricordano che i trasferimenti derivanti dalla connessione e dall'uso di MyHealth@EU e HealthData@EU dovrebbero rispettare il capo V GDPR.

116. In particolare EDPB e GEPD osservano che tanto l'articolo 13, paragrafo 3, quanto l'articolo 52, paragrafo 5, della proposta, fanno riferimento ai controlli di conformità che la Commissione deve effettuare prima di emettere l'atto di esecuzione che stabilisce che un punto di contatto nazionale di

---

[37] Articolo 48 GDPR: "[l]e sentenze di un'autorità giurisdizionale e le decisioni di un'autorità amministrativa di un paese terzo che dispongono il trasferimento o la comunicazione di dati personali da parte di un titolare del trattamento o di un responsabile del trattamento possono essere riconosciute o assumere qualsivoglia carattere esecutivo soltanto se basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro, ad esempio un trattato di mutua assistenza giudiziaria, fatti salvi gli altri presupposti di trasferimento a norma del presente capo".

[38] A tale proposito il considerando 78 GDPR prevede che "[i] principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici". Inoltre il considerando 77 della direttiva 2014/24/UE sugli appalti pubblici prevede che "[n]el redigere le specifiche tecniche, le amministrazioni aggiudicatrici dovrebbero tener conto dei requisiti derivanti dal diritto dell'Unione in materia di protezione dei dati, in particolare per quanto riguarda la progettazione del trattamento dei dati personali (protezione dei dati fin dalla progettazione)".

un terzo Il paese o un sistema istituito a livello internazionale è conforme ai requisiti di MyHealth@EU o HealthData@EU. EDPB e GEPD osservano altresì che il considerando 26 della proposta, relativo a MyHealth@EU, menziona la necessità di tali controlli per garantire "la conformità del punto di contatto nazionale alle specifiche tecniche, alle norme in materia di protezione dei dati e ad altre prescrizioni [...]". **A tale proposito, EDPB e GEPD raccomandano di chiarire direttamente tanto nell'articolo 13, paragrafo 3, quanto nell'articolo 52, paragrafo 5, della proposta che i controlli di conformità dovrebbero garantire il rispetto del capo V GDPR una volta che il punto di contatto nazionale di un paese terzo o un sistema istituito a livello internazionale sarà connesso a MyHealth@EU o HealthData@EU.**

9 GOVERNANCE E COORDINAMENTO EUROPEI (CAPO VI)

117. EDPB e GEPD osservano che l'articolo 64 della proposta istituisce il comitato dello spazio europeo dei dati sanitari (comitato EHDS)**,** un organo di coordinamento che mira ad agevolare la cooperazione e lo scambio di informazioni tra gli Stati membri. EDPB e GEPD rilevano che il comitato EHDS sarà composto da rappresentanti delle autorità di sanità digitale e degli organismi responsabili dell'accesso ai dati sanitari di tutti gli Stati membri e che **il comitato EHDS sarà presieduto dalla Commissione.** EDPB e GEPD osservano che, in linea con la proposta, i rappresentanti di EDPB e GEPD possono essere invitati alle riunioni qualora siano discusse questioni in materia di protezione dei dati. **EDPB e GEPD ritengono che i loro rappresentanti dovrebbero essere membri permanenti del comitato EHDS (pertanto non soltanto potenzialmente invitati a partecipare) e dovrebbero partecipare a tutte le discussioni concernenti questioni in materia di protezione dei dati personali**, al fine di garantire un'interpretazione e un'applicazione coerenti delle disposizioni introdotte dalla proposta in merito alle disposizioni del GDPR.

118. Inoltre l'articolo 65, paragrafo 1, della proposta definisce i compiti del comitato EHDS sull'uso primario dei dati sanitari elettronici. EDPB e GEPD rilevano che la Commissione potrà emettere contributi scritti e scambiare le migliori pratiche in merito a questioni relative all'attuazione della proposta, in particolare in relazione alle disposizioni di cui ai capi II e III della proposta (articolo 65, paragrafo 1, lettera b), punto i)) e a qualsiasi aspetto dell'uso primario dei dati sanitari elettronici (articolo 65, paragrafo 1, lettera b), punto iii)). Poiché il capo II della proposta prevede diritti alla protezione dei dati analoghi a quelli del GDPR (cfr. punto 28), EDPB e GEPD ritengono che il comitato EHDS non dovrebbe poter essere in grado di emettere contributi scritti relativi a questioni concernenti diritti di protezione dei dati. In caso contrario, **EDPB e GEPD sottolineano che la proposta rischia di introdurre una divergenza nell'interpretazione o nell'applicazione dei diritti alla protezione dei dati** stabiliti da EDPB e GEPD. Inoltre EDPB e GEPD osservano che tale disposizione creerà incertezza del diritto, che sarà altresì in contraddizione con gli obiettivi della proposta concernenti il miglioramento del funzionamento del mercato interno **stabilendo un quadro giuridico uniforme** (considerando 1 della proposta). Inoltre l'articolo 65, paragrafo 2, della proposta specifica i compiti del comitato EHDS relativi all'uso secondario dei dati sanitari elettronici. EDPB e GEPD ribadiscono il loro avvertimento in merito alle competenze del comitato EHDS in merito alla pubblicazione di contributi scritti concernenti questioni relative a diritti alla protezione dei dati per quanto riguarda l'uso secondario dei dati sanitari elettronici.

119. Inoltre, ai sensi dell'articolo 65, paragrafo 1, lettera d), e dell'articolo 65, paragrafo 2, lettera d), della proposta, EDPB e GEPD rilevano che il comitato EHDS potrà condividere informazioni sui rischi e sugli

incidenti in materia di protezione dei dati relativi all'uso primario e secondario dei dati sanitari elettronici, nonché sulla gestione di tali rischi e incidenti. **Ancora una volta EDPB e GEPD sottolineano che la proposta rischia di introdurre una divergenza tra l'EDPB, il GEPD e il comitato EHDS per quanto concerne l'individuazione o la gestione di violazioni dei dati**, poiché il comitato EHDS sarà in grado di condividere informazioni sulle possibili modalità di gestione di incidenti in materia di protezione dei dati. Inoltre non vi è chiarezza in merito ai destinatari delle informazioni che il comitato EHDS condividerà. Più in generale EDPB e GEPD raccomandano al co-legislatore di specificare l'interazione tra EDPB, GEPD e comitato EHDS in merito alle questioni in materia di protezione dei dati che dovrebbero rimanere di competenza esclusiva delle autorità di protezione dei dati.

120. Per quanto concerne il medesimo capo, EDPB e GEPD osservano che l'articolo 66 della proposta afferma che la Commissione deve istituire due gruppi incaricati di provvedere al controllo congiunto delle infrastrutture transfrontaliere MyHealth@EU e HealthData@EU (articoli 12 e 52 della proposta). **EDPB e GEPD osservano che l'ambito di applicazione dei compiti dei gruppi incaricati di provvedere al controllo congiunto non è definito in maniera chiara e che possono sovrapporsi ai compiti del comitato EHDS** ai sensi dell'articolo 65 della proposta. Più in generale EDPB e GEPD raccomandano che l'interazione tra organi, gruppi e organizzazioni diversi menzionati nella proposta sia definita in maniera chiara.

121. Inoltre EDPB e GEPD rilevano alcune incoerenze tra i compiti dei sottogruppi e il potere della Commissione di adottare atti di esecuzione o delegati in merito ai medesimi argomenti. Ad esempio, ai sensi dell'articolo 52, paragrafo 13, della proposta, la Commissione può stabilire prescrizioni, specifiche tecniche, architettura informatica di HealthData@EU attraverso atti di esecuzione, ma anche uno dei due sottogruppi adotterà decisioni riguardanti lo sviluppo e il funzionamento della medesima infrastruttura. **Di conseguenza EDPB e GEPD raccomandano di chiarire l'interazione tra la Commissione e tali sottogruppi.**

10 DELEGA E COMITATO (CAPO VII)

122. Il capo VII della proposta consente alla Commissione di adottare atti delegati in merito a diversi aspetti concreti disciplinati dalla proposta. A questo proposito, EDPB e GEPD osservano che, indipendentemente dal coinvolgimento degli Stati membri nel processo decisionale, il potere di decidere di modificare o estendere alcune delle questioni essenziali affrontate dalla proposta lascia ancora alla Commissione un notevole margine di manovra per modificare o estendere l'ambito di applicazione della proposta stessa in un modo suscettibile di incidere sui diritti alla protezione dei dati e sulla competenza esclusiva degli Stati membri di definire le loro politiche sanitarie nazionali.

123. In particolare EDPB e GEPD ritengono che l'articolo 5, paragrafo 2, e l'articolo 33, paragrafo 7, della proposta destino preoccupazioni, in quanto alla Commissione è conferito il potere di modificare l'elenco delle categorie prioritarie di dati sanitari elettronici a cui si accede e scambiati negli Stati membri per l'uso primario così come l'elenco dei dati sanitari elettronici, fatti salvi la messa a disposizione obbligatoria e l'accesso obbligatorio da parte di terzi per l'uso secondario. Poiché qualsiasi modifica di tali categorie di dati personali, segnatamente delle categorie particolari di dati, potrebbe richiedere una rivalutazione dei rischi per i diritti e gli interessi fondamentali delle persone interessate, queste questioni equivalgono a questioni sostanziali che dovrebbero essere considerate elementi essenziali, ai sensi dell'articolo 290 del TFUE.

124. Di conseguenza EDPB e GEPD ritengono che tali questioni non dovrebbero essere escluse dal livello legislativo, nel contesto del quale qualsiasi limitazione dei diritti fondamentali dovrebbe essere chiaramente prevista ai fini del conseguimento dell'indispensabile prevedibilità dello strumento giuridico, mentre solo campi di dati più dettagliati (sottocategorie di dati) che rientrano nelle categorie già definite di dati stabilite all'articolo 5, paragrafo 1, e all'articolo 33, paragrafo 1, della proposta dovrebbero essere aggiunti attraverso l'adozione di atti delegati.

125. Inoltre EDPB e GEPD osservano che i criteri previsti dall'articolo 5, paragrafo 2, lettera b), della proposta per guidare la Commissione nel decidere le categorie prioritarie di dati sanitari elettronici da aggiungere all'elenco stabilito all'articolo 5, paragrafo 1, della proposta, sembrano vaghi e dovrebbero essere ulteriormente delimitati[39].

126. Infine, anche se l'articolo 67, paragrafo 4, della proposta, afferma che la Commissione deve consultare gli esperti designati da ciascuno Stato membro che possono comportare competenze in questioni concernenti la protezione dei dati, EDPB e GEPD raccomandano di introdurre un riferimento chiaro all'articolo 42 EUDPR per chiarire che GEPD ed EDPB devono essere consultati se del caso quando vengono proposti tali atti delegati.

11 VARIE (CAPO VIII)

127. EDPB e GEPD rilevano che il capo VIII della proposta assegna agli Stati membri dell'UE la competenza per la definizione delle sanzioni applicabili alle violazioni del regolamento. EDPB e GEPD ritengono che ciò potrebbe potenzialmente portare a significative incertezze del diritto rispetto alla corretta applicazione delle norme stabilite dalla proposta in Stati membri diversi, in ragione della diversa determinazione della portata delle sanzioni, che potrebbero risultare in importi minimi e massimi significativamente diversi applicati da uno Stato membro rispetto a un altro. A questo proposito, EDPB e GEPD rilevano che dovrebbero essere stabilite norme armonizzate in materia di sanzioni al fine di garantire un'applicazione equa e sicura, in particolare nel contesto di casi transfrontalieri.

128. Infine EDPB e GEPD osservano che, in linea con le precedenti osservazioni in materia di autocertificazione dei sistemi di cartelle cliniche elettroniche, i termini di valutazione e riesame stabiliti ai sensi dell'articolo 70 della proposta sono troppo lunghi per garantire un'attuazione corretta e tempestiva.

[39] I criteri fanno riferimento alla "categoria [...] utilizzata in un numero significativo di sistemi di cartelle cliniche elettroniche impiegati negli Stati membri" secondo le informazioni più recenti.

Per il Garante europeo della protezione dei dati Il Garante europeo della protezione dei dati (Wojciech Wiewiorowski)	Per il comitato europeo per la protezione dei dati La presidente (Andrea Jelinek)

[1] Ad esempio non è chiaro se i fabbricanti rientrino in tale categorizzazione.