



17 / IT

WP260 Rev.01

Gruppo dell'articolo 29

Linee guida in materia di trasparenza ai sensi del regolamento 2016/679

Adottato il 29 novembre 2017

Riveduta da ultimo e adottato il 11 aprile 2018

IL GRUPPO DI LAVORO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL

TRATTAMENTO DEI DATI PERSONALI

istituito dalla direttiva 95/46 / CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995,

visti gli articoli 29 e 30,

visto il suo regolamento,

Avrà adottato gli orientamenti presenti:

Questo gruppo di lavoro è stato istituito ai sensi dell'articolo 29 della direttiva 95/46 / CE. Si tratta di un organo consultivo indipendente dell'UE per la protezione dei dati e della privacy. I suoi compiti sono letto descr all'articolo 30 della direttiva 95/46 / CE e all'articolo 15 della direttiva 2002/58 / CE.

La segreteria è fornito dalla Direzione C (Diritti fondamentali e cittadinanza dell'Unione) della Commissione europea, Direzione generale Giustizia, B-1049 Bruxelles, Belgio, Ufficio MO-59 02/013.

Sito web: <http://ec.europa.eu/newsroom/article29/news.cfm?item type = 1358 & tpa id = 6936>



Sommario

Introduzione	4
Il significato di trasparenza	6
Elementi di trasparenza sotto la GDPR	6
<i>"Concisa, trasparente, comprensibile e facilmente accessibile"</i>	<i>7</i>
<i>"Linguaggio chiaro e semplice"</i>	<i>8</i>
<i>Fornire informazioni ai bambini e altre persone vulnerabili</i>	<i>10</i>
<i>"per iscritto o con altri mezzi"</i>	<i>11</i>
<i>"..il informazioni possono essere fornite oralmente"</i>	<i>12</i>
<i>"Gratuito"</i>	<i>13</i>
Informazioni da fornire alla persona interessata - gli articoli 13 e 14	13
<i>Soddisfare</i>	<i>13</i>
<i>"misure appropriate"</i>	<i>14</i>
<i>Timing per la fornitura di informazioni</i>	<i>14</i>
<i>Modifiche all'articolo 13 e all'articolo 14, le informazioni</i>	<i>16</i>
<i>Timing di notifica delle modifiche all'articolo 13 e all'articolo 14 Informazioni</i>	<i>17</i>
<i>Modalità - Formato di fornitura di informazioni</i>	<i>18</i>
<i>approccio a più livelli in un ambiente digitale e stratificate normative sulla privacy / comunicazioni</i>	<i>19</i>
<i>approccio stratificato in un ambiente non digitale</i>	<i>20</i>
<i>"Push" e le comunicazioni "pull"</i>	<i>20</i>
<i>Altri tipi di "misure appropriate"</i>	<i>21</i>
<i>Informazioni sul profiling e il processo decisionale automatizzato</i>	<i>22</i>
<i>Altre questioni - rischi, le regole e le garanzie</i>	<i>22</i>
Informazioni relative a ulteriori elaborazioni	23
strumenti di visualizzazione	25
<i>Icone</i>	<i>25</i>
<i>meccanismi di certificazione, sigilli e segni</i>	<i>26</i>
Esercizio dei diritti degli interessati	26
Eccezioni all'obbligo di fornire informazioni	27
<i>Articolo 13 eccezioni</i>	<i>27</i>
<i>Articolo 14 eccezioni</i>	<i>28</i>

<i>Si rivela impossibile, sforzo sproporzionato e seria compromissione degli obiettivi</i>	28
<i>"Rivela impossibile"</i>	29
<i>Impossibilità di fornire la fonte dei dati</i>	29
<i>"Sforzo sproporzionato"</i>	30
<i>compromissione grave degli obiettivi</i>	31
<i>Ottenere o divulgazione è espressamente prevista dalla legge</i>	32
<i>Riservatezza in virtù di un obbligo segretezza</i>	33
Restrizioni al diritto di dati soggetti	33
Trasparenza e violazioni dei dati	34
Allegato	35



introduzione

1. Queste linee guida forniscono una guida pratica e assistenza interpretativa dal Partito di lavoro articolo 29 (WP29) sul nuovo obbligo di trasparenza relativa al trattamento dei dati personali ai sensi del regolamento generale sulla protezione dei dati¹, il " GDPR "). **La trasparenza è un obbligo generale sotto il GDPR applicare a tre centrali le zone : (1) la fornitura di informazioni alle persone interessate relativi al trattamento equo; (2) come i titolari del trattamento comunicano con le persone interessate in relazione ai loro diritti ai sensi della GDPR; e (3) come i titolari del trattamento agevolare l'esercizio da parte di soggetti di dati dei loro diritti². Nella misura in cui il rispetto della trasparenza è richiesta in relazione al trattamento dei dati ai sensi della direttiva (UE) 2016/680³, queste linee guida si applicano anche all'interpretazione di tale principio.** ⁴ Queste linee guida sono, come tutti i WP29 linee guida, destinati ad essere generalmente applicabili e pertinenti per i controllori indipendentemente dal settore, l'industria o le specifiche normative particolare qualsiasi titolare del trattamento. In quanto tali, queste linee guida non possono affrontare le sfumature e le numerose variabili che possono sorgere nel contesto degli obblighi di trasparenza di un settore specifico, l'industria o area regolamentato. Tuttavia, queste linee guida hanno lo scopo di consentire ai controllori di capire, ad alto livello, l'interpretazione di WP29 di ciò che gli obblighi di trasparenza comportano nella pratica e per indicare l'approccio che WP29 considera regolatori dovrebbero prendere ad essere trasparente mentre incorporando l'equità e responsabilità nelle loro misure di trasparenza .

2. **La trasparenza è una caratteristica di lunga data della legge dell'UE⁵. Si tratta di generare fiducia nei processi che interessano il cittadino, consentendo loro di capire, e, se necessario, sfidare quei processi. È anche espressione del principio di equità in relazione al**

¹ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla tutela 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 .

² Queste linee guida di cui i principi generali in relazione all'esercizio dei diritti degli interessati piuttosto che considerare le modalità specifiche per ciascuno dei singoli diritti della persona sotto la GDPR.

³ Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016 sul la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini della prevenzione, ricerca, accertamento e perseguimento di penale reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, e che abroga la decisione quadro 2008/977 / GAI del Consiglio

⁴ Mentre la trasparenza non è uno dei principi in materia di trattamento dei dati personali di cui all'articolo 4 della direttiva (UE) 2016/680, considerando 26 Stati che qualsiasi trattamento di dati personali deve essere "legale, equo e trasparente" in relazione alla persone fisiche interessate.

⁵ L'articolo 1 del TUE si riferisce alle decisioni prese " *nel modo più trasparente possibile e il più vicino al cittadino il più possibile* "; L'articolo 11 (2) afferma che " *Le istituzioni mantengono un dialogo aperto, trasparente e regolare con le associazioni rappresentative e la società civile* "; e l'articolo 15 del TFUE si riferisce tra l'altro per i cittadini dell'Unione hanno il diritto di accedere ai documenti delle istituzioni, organi, uffici e agenzie e ai requisiti di queste istituzioni, organi, uffici e agenzie per garantire che le loro procedure siano trasparente.

trattamento dei dati personali ha espresso dall'articolo 8 della Carta dei diritti fondamentali dell'Unione europea. **Sotto la GDPR (articolo 5 (1) (a))⁶, oltre ai requisiti che devono essere trattati dati lecito e secondo correttezza, trasparenza viene ora incluso come un aspetto fondamentale di tali principi.⁷ La trasparenza è intrinsecamente legata alla correttezza e al nuovo principio di responsabilità sotto il GDPR. Risulta inoltre da articolo 5.2 che il controllore deve sempre essere in grado di dimostrare che i dati personali sono trattati in modo trasparente rispetto alla persona.⁸ Collegato a questo, il principio di responsabilità richiede trasparenza delle operazioni di trattamento, in modo che i titolari del trattamento sono in grado di dimostrare la conformità con i loro obblighi ai sensi della GDPR⁹.**

3. In conformità del considerando 171 del GDPR, quando il trattamento è già in corso prima del 25 maggio 2018, un controllore di dati deve garantire che sia conforme agli obblighi trasparenza del 25 maggio 2018 (insieme a tutti gli altri obblighi a norma GDPR). Ciò significa che prima del 25 maggio 2018, responsabili del trattamento dovrebbero rivedere tutte le informazioni fornite alle persone relative al trattamento dei dati personali (ad esempio in normative sulla privacy / comunicazioni etc.) per garantire che rispettano i requisiti relativi alla trasparenza che sono discusso in queste linee guida. Dove vengono apportate modifiche o aggiunte a tali informazioni, controllori devono far capire alle persone che questi cambiamenti sono stati effettuati per conformarsi con la GDPR. WP29 raccomanda che tali modifiche o integrazioni attivamente portate all'attenzione delle persone interessate, ma ad un controller minime dovrebbero rendere queste informazioni pubblicamente disponibili (ad esempio sul loro sito web). Tuttavia, se le modifiche o aggiunte sono materiale o sostanziale, quindi in linea con i paragrafi da 29 a 32 qui sotto, tali modifiche devono essere portate attivamente l'attenzione della persona.
4. Trasparenza, quando rispettate da responsabili del trattamento, autorizza interessati per tenere controllori e elaboratori di dati affidabile e di esercitare controllo sui propri dati personali, per esempio, fornendo o ritirare il **consenso informato e actioning loro dati diritti soggetti**¹⁰. Il concetto di trasparenza nel GDPR è user-centric piuttosto che legalista ed è realizzata per mezzo di specifiche esigenze pratiche sui controllori e processori di dati in una serie di articoli. I pratici requisiti (informazioni) sono descritte negli articoli 12 - 14 del GDPR. Tuttavia, la qualità, l'accessibilità e la comprensibilità delle informazioni è importante quanto il contenuto effettivo delle informazioni di trasparenza, che devono essere fornite agli interessati.

⁶ "I dati personali sono trattati in modo lecito, secondo correttezza e in modo trasparente rispetto alla persona".

⁷ Nella direttiva 95/46 / CE, la trasparenza si alludeva solo al considerando 38 per mezzo di un requisito per l'elaborazione dei dati per essere onesti, ma non espressamente fatto riferimento nel equivalente all'articolo 6 (1) (a).

⁸ L'articolo 5.2 del GDPR obbliga un controllore dei dati per dimostrare la trasparenza (insieme agli altri cinque principi in materia di trattamento dei dati di cui all'articolo 5.1) in base al principio di responsabilità.

⁹ L'obbligo per i titolari del trattamento di attuare misure tecniche ed organizzative per garantire ed essere in grado di dimostrare che il trattamento viene eseguito in conformità con la GDPR è di cui all'articolo 24.1.

¹⁰ Si veda, ad esempio, le conclusioni dell'avvocato generale Cruz Villalon (9 luglio 2015) nel caso Bara (causa C-201/14) al punto 74: "l'obbligo di informare le persone interessate in merito al trattamento dei dati personali, che garantisce la trasparenza di tutti i trattamenti, è tanto più importante poiché incide l'esercizio, da persone interessate del loro diritto di accesso ai dati da elaborare, di cui l'articolo 12 della direttiva 95/46, e il diritto di opporsi al trattamento di tali dati, di cui all'articolo 14 di tale direttiva".

5. Gli obblighi di trasparenza del GDPR applicano a prescindere dalla base giuridica per l'elaborazione e per tutto il ciclo di vita di lavorazione. Questo emerge dal l'articolo 12 che prevede che la trasparenza si applica al seguente stadi del ciclo di trattamento:

- prima o all'inizio del ciclo di trattamento, cioè quando i dati personali vengono raccolti sia presso l'interessato o altrimenti ottenute;
- per tutto il periodo di elaborazione, cioè quando si comunica con persone interessate sui loro diritti; e
- in punti specifici durante l'elaborazione è in corso, per esempio quando si verificano violazioni di dati o in caso di modifiche sostanziali al trattamento.

Il significato di trasparenza

6. La trasparenza non è definito nel GDPR. Considerando 39 della GDPR è informativo sul significato e l'effetto del principio di trasparenza nel contesto del trattamento dei dati:

“Dovrebbe essere trasparente alle persone fisiche che i loro dati personali sono raccolti, utilizzati, consultati o altrimenti elaborati e in che misura i dati personali sono o saranno elaborati. Il principio di trasparenza richiede che le informazioni e la comunicazione relativa al trattamento dei dati personali coloro essere facilmente accessibili e di facile comprensione, e possono essere usate che un linguaggio chiaro e semplice. Tale principio riguarda, in particolare, le informazioni agli interessati sull'identità del programmatore e gli scopi del trattamento e ulteriori informazioni per assicurare un trattamento equo e trasparente nei confronti delle persone fisiche interessate ed il diritto di ottenere la conferma e comunicazione personale che sono in fase di elaborazione dati che li riguardano ...”

Elementi di trasparenza sotto la GDPR

7. Gli articoli chiave in relazione alla trasparenza nel GDPR, come si applicano ai diritti della persona interessata, si trovano nel capitolo III (diritti della persona interessata). Articolo 12 stabilisce le regole generali che si applicano a: la fornitura di informazioni alle persone interessate (ai sensi degli articoli 13

- 14); le comunicazioni con gli interessati che regolano l'esercizio dei loro diritti (ai sensi degli articoli 15 - 22); e le comunicazioni in relazione alle violazioni dei dati (articolo 34). In particolare l'articolo 12 richiede che le informazioni o la comunicazione in questione devono rispettare le seguenti regole:

- deve essere conciso, trasparente, comprensibile e facilmente accessibile (articolo 12.1);
- linguaggio chiaro e semplice deve essere utilizzato (articolo 12.1);
- l'esigenza di un linguaggio chiaro e semplice è di particolare importanza nel fornire informazioni ai bambini (articolo 12.1);
- essa deve essere in forma scritta *“O con altri mezzi, con, eventualmente, per via elettronica”* (Articolo 12.1);
- ove richiesto dal soggetto dati che può essere fornita verbalmente (articolo 12.1); e

- generalmente deve essere fornita gratuitamente (articolo 12.5).

"Concisa, trasparente, comprensibile e facilmente accessibile"

8. Il requisito che la fornitura di informazione e comunicazione con, interessati avviene in maniera "sintetica e trasparente" indica che i titolari devono presentare le informazioni / comunicazione efficiente e sintetico per evitare informazioni faticose. Queste informazioni dovrebbero essere chiaramente differenziate da altre informazioni relative non privacy quali le disposizioni contrattuali o condizioni generali di utilizzo. In un contesto in linea, l'uso di una dichiarazione a strati privacy / avviso consentirà un soggetto di dati per navigare alla particolare sezione della dichiarazione sulla privacy / avviso che vogliono accedere immediatamente invece di dover scorrere grandi quantità di testo alla ricerca di particolari problemi.
9. Il requisito che l'informazione è "intelligibile" significa che dovrebbe essere compreso da un componente medio del destinatario. L'intelligibilità è strettamente legata alla necessità di utilizzare un linguaggio chiaro e semplice. Un controller di dati responsabile avrà conoscenza circa le persone che raccolgono informazioni su e si può usare questa conoscenza per determinare quali quel pubblico sarebbe probabilmente capire. Ad esempio, un controllore raccolta dei dati personali di lavorare i professionisti possono assumere il suo pubblico ha un alto livello di comprensione di un controller che ottiene i dati personali dei bambini. Se i controller sono incerti circa il livello di intelligibilità e la trasparenza delle informazioni e l'efficacia delle interfacce utente / comunicazioni / politiche, ecc, possono testare questi, ad esempio, attraverso meccanismi come i pannelli di utente,
10. Una considerazione fondamentale del principio della trasparenza illustrato in queste disposizioni è che la persona interessata dovrebbe essere in grado di determinare in anticipo quale la portata e le conseguenze del trattamento comporta e che non dovrebbero essere prese di sorpresa in un momento successivo sui modi in i loro dati personali è stato utilizzato. Anche questo è un aspetto importante del principio di equità ai sensi dell'articolo 5.1 del GDPR e in effetti è collegata al considerando 39 che stabilisce che *"[N] persone atural dovrebbero essere consapevoli dei rischi, regole, tutele e diritti in relazione al trattamento dei dati personali ..."* In particolare, per l'elaborazione di dati complessi, tecnici o inatteso, la posizione di WP29 è che, oltre a fornire le informazioni prescritte ai sensi degli articoli 13 e 14 (trattati più avanti in queste linee guida), i controllori dovrebbero anche separatamente precisare in un linguaggio inequivocabile ciò **che il più importante conseguenze del trattamento sarà: in altre parole, che tipo di effetto avrà trattamento specifico** descritto in una dichiarazione sulla privacy / preavviso effettivamente avere su un argomento di dati? In conformità con il principio di responsabilità e in linea con il considerando 39, responsabili del trattamento devono valutare se esistono particolari rischi per persone fisiche coinvolte in questo tipo di lavorazione che deve essere portato a conoscenza degli interessati. Questo può aiutare a fornire una panoramica dei metodi di trattamento che potrebbero avere il massimo impatto sui diritti e le libertà delle persone fondamentali in relazione alla protezione dei loro dati personali.

11. L'elemento "facilmente accessibile" significa che la persona interessata non dovrebbe avere a cercare le informazioni; dovrebbe essere immediatamente evidente a loro dove e come queste informazioni si può accedere, ad esempio fornendo direttamente a loro, collegandoli ad essa, da che indichi chiaramente o come una risposta ad una domanda del linguaggio naturale (ad esempio in una linea informativa sulla privacy stratificato / preavviso, in domande frequenti, a titolo di contestuali pop-up che attivano quando un soggetto di dati attraverso il formulario on-line, o in un contesto digitale interattivo attraverso un'interfaccia chatbot, ecc. Questi meccanismi sono più considerati di seguito, anche a paragrafi da 33 a 40).

Esempio

Ogni organizzazione che gestisce un sito web dovrebbe pubblicare una dichiarazione sulla privacy / avviso sul sito. Un link diretto a questa informativa sulla privacy / avviso deve essere chiaramente visibile in ogni pagina di questo sito web sotto un termine comunemente usato (come "Privacy", "Privacy Policy" o "privacy Policy"). Schemi di posizionamento o di colori che rendono un testo o un collegamento meno evidente, o difficili da trovare su una pagina web, non sono considerati facilmente accessibili.

Per le applicazioni, le informazioni necessarie devono anche essere messa a disposizione da un negozio online prima del download. Una volta che l'applicazione è installata, l'informazione deve ancora essere facilmente accessibile da dentro l'applicazione. Un modo per soddisfare questo requisito è quello di garantire che le informazioni siano mai più di "due tocchi di distanza" (ad esempio, includendo un "Privacy" / opzione "protezione dei dati" nel menu di funzionalità della app). Inoltre, l'informativa sulla privacy in questione dovrebbe essere specifico per l'applicazione particolare e non deve essere semplicemente l'informativa sulla privacy generica della società che possiede l'applicazione o lo rende disponibile al pubblico.

WP29 raccomanda come una best practice che al momento della raccolta dei dati personali in un contesto online viene fornito un link alla informativa sulla privacy / preavviso o che queste informazioni sono rese disponibili sulla stessa pagina in cui vengono raccolti i dati personali.

"Linguaggio chiaro e semplice"

12. Con **scritto** informazioni (e le informazioni in cui scritte è resa oralmente, o con metodi audiovisivi audio /, tra cui per gli interessati ipovedenti), le migliori pratiche per la scrittura chiara devono essere seguite.¹¹ Un requisito linguaggio simile (per "chiaro e comprensibile") è stato usato in precedenza dal legislatore comunitario¹² ed è anche esplicitamente cui nel contesto di consenso nel considerando 42 del GDPR¹³. L'esigenza di linguaggio chiaro e semplice significa che le informazioni dovrebbero essere fornite in semplice modo possibile, evitando strutture sintattiche e linguistiche complesse. L'informazione dovrebbe essere concreto e definitivo; non dovrebbe essere formulata in termini astratti o ambivalenti o lasciare spazio per i diversi

¹¹ Vedere Come scrivere in modo chiaro da la Commissione europea (2011), essere Trovato a: <https://publications.europa.eu/en/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5>.

¹² L'articolo 5 della direttiva 93/13 / CEE del Consiglio, del 5 aprile 1993 concernente le clausole abusive nei contratti dei consumatori

¹³ Considerando 42 stabilisce che una dichiarazione di consenso pre-formulata da un controllore dati devono essere forniti in forma comprensibile e facilmente accessibile, utilizzando linguaggio chiaro e semplice e non dovrebbe contenere clausole abusive.

interpretazioni. In particolare, ai fini della, e la base giuridica per, il trattamento dei dati personali devono essere chiari.

Esempi cattive pratiche

Le seguenti frasi non sono sufficientemente chiare sulle finalità del trattamento:

- *“Potremmo utilizzare i tuoi dati per sviluppare nuovi servizi”* (come non è chiaro quello che i “servizi” sono o come i dati contribuiranno a sviluppare loro);
- *“Possiamo utilizzare i vostri dati personali per scopi di ricerca”* (come non è chiaro che tipo di “ricerca” si riferisce a); e
- *“Potremmo utilizzare i tuoi dati per offrire servizi personalizzati”* (come non è chiaro quale comporta la “personalizzazione”).

Esempi di buone pratiche¹⁴

- *“Conserveremo la vostra storia dello shopping e utilizzare i dettagli dei prodotti che avete precedentemente acquistato a dare suggerimenti a voi per gli altri prodotti che riteniamo sarà anche interessato a”* (è chiaro che quali tipi di dati verranno trattati, che la persona sarà oggetto di pubblicità mirata per i prodotti e che i loro dati saranno utilizzati per abilitare questa);
- *“Conserveremo e valutare le informazioni sulle recenti visite al nostro sito Web e come ci si sposta in giro per diverse sezioni del nostro sito web per scopi di analisi per capire come le persone utilizzano il nostro sito web in modo che possiamo rendere più intuitivo”* (è chiaro quale tipo di dati saranno elaborati e il tipo di analisi che il controllore sta per intraprendere); e
- *“Noi tenere un registro degli articoli sul nostro sito web che avete cliccato su e utilizzare tali informazioni per indirizzare la pubblicità su questo sito che è rilevante per i vostri interessi, che abbiamo identificato sulla base di articoli che avete letto”* (è chiaro che cosa la personalizzazione comporta e come sono stati individuati gli interessi attribuiti alla persona).

13. qualificazioni linguistiche quali “può”, “potrebbe”, “alcuni”, “spesso” e “possibile” dovrebbe anche essere evitata. Dove i titolari del trattamento scelgono di usare il linguaggio indefinito, dovrebbero essere in grado, in base al principio di responsabilità, per dimostrare il motivo per cui l'uso di tale lingua non potrebbe essere evitato e come non pregiudichi l'equità del trattamento. I paragrafi e le frasi devono essere ben strutturate, utilizzando proiettili ei rientri da segnalare gerarchica

¹⁴ L'esigenza di trasparenza sussiste anche indipendentemente da requisito momento responsabili del trattamento per garantire che vi sia una base giuridica adeguata per il trattamento di cui all'articolo 6.

relazioni. La scrittura deve essere in attivo invece della forma passiva e sostantivi in eccesso deve essere evitato. Le informazioni fornite a un soggetto di dati non dovrebbe contenere eccessivamente legalista linguaggio, tecnico o di uno specialista o di terminologia. Quando l'informazione viene tradotta in una o più lingue, il titolare del trattamento deve garantire che tutte le traduzioni siano accurate e che la fraseologia e la sintassi ha senso nella seconda lingua (s) in modo che il testo tradotto non deve essere decifrato o reinterpretato. (Una traduzione in una o più altre lingue dovrebbero essere fornite in cui gli obiettivi del controller¹⁵

interessati che parlano quelle lingue.)

Fornire informazioni ai bambini e altre persone vulnerabili

14. **Se un controllore dei dati si rivolge bambini¹⁶ o è, o dovrebbe essere, consapevoli del fatto che i loro prodotti / servizi sono particolarmente utilizzati dai bambini (tra cui in cui il controller si basa sul consenso del minore)¹⁷, si dovrebbe assicurare che il vocabolario, tono e lo stile del linguaggio usato è opportuno e risuona con i bambini in modo che il destinatario bambino delle informazioni riconosce che il messaggio / informazioni è diretto contro di loro.¹⁸ Un utile esempio di linguaggio centrata sul bambino usato come alternativa al linguaggio giuridico originale si trova nella "Convenzione delle Nazioni Unite sui diritti del fanciullo in Bambini benvenuti Language".¹⁹**
15. La posizione di WP29 è che la trasparenza è un diritto autonomo che si applica tanto ai bambini come si fa per gli adulti. WP29 sottolinea in particolare che i bambini non perdono i loro diritti in qualità di alla trasparenza, semplicemente perché il consenso è stato dato / autorizzato dal titolare della responsabilità genitoriale in una situazione di cui all'articolo 8 del GDPR applica. Mentre tale consenso sarà, in molti casi, essere dato o autorizzato su base una tantum da parte del titolare della responsabilità genitoriale, un bambino (come ogni altro interessato) ha un diritto in corso alla trasparenza in tutto il continuum di loro impegno con un data controller. Ciò è coerente con l'articolo 13 della Convenzione delle Nazioni Unite sui diritti del fanciullo, che afferma che un **bambino ha diritto alla libertà di espressione, che comprende il diritto di cercare,²⁰ E 'importante sottolineare che, pur prevedendo il consenso da dare conto di un bambino quando in una determinata età,²¹ Articolo 8 non fornisce per misure di trasparenza per essere indirizzati al titolare della responsabilità genitoriale che**

¹⁵ Ad esempio, in cui il controller gestisce un sito web nella lingua in questione e / o offre opzioni specifiche per paese e / o facilita il pagamento di beni o servizi nella valuta di un determinato Stato membro, allora questi può essere indicativo di un dato trattamento dei dati mira soggetti di un particolare stato membro.

¹⁶ Il termine "bambino" non è definito sotto il GDPR, tuttavia WP29 riconosce che, in conformità con la Convenzione delle Nazioni Unite sui diritti del fanciullo, che tutti gli Stati membri dell'UE hanno ratificato, un bambino è una persona di età inferiore ai 18 anni.

¹⁷ cioè i bambini di 16 anni o più anziani (o, se ai sensi dell'articolo 8.1 del diritto nazionale GDPR Stato membro ha fissato l'età del consenso ad una determinata età compresa tra i 13 ei 16 anni per i bambini di consentire ad un'offerta per la fornitura di informazioni servizi della società, i bambini che si incontrano che l'età del consenso nazionale).

¹⁸ Il considerando 38 afferma che "I bambini meritano una protezione speciale per quanto riguarda i propri dati personali in quanto potrebbero essere meno consapevoli dei rischi, le conseguenze e le garanzie in questione e dei loro diritti in relazione al trattamento dei dati personali". Il considerando 58 afferma che "Dato che i bambini meritano una protezione specifica, tutte le informazioni e la comunicazione, in cui l'elaborazione è rivolto a un bambino, dovrebbe essere in una lingua così chiaro e semplice che il bambino può facilmente capire".

¹⁹ <https://www.unicef.org/rightsite/files/uncrcchildfriendlylanguage.pdf>

²⁰ L'articolo 13 della Convenzione delle Nazioni Unite sui diritti del fanciullo stabilisce che: "Il fanciullo ha diritto alla libertà di espressione; tale diritto comprende la libertà di cercare, ricevere e diffondere informazioni e idee di ogni genere, senza riguardo a frontiere, oralmente, per iscritto oa mezzo stampa o in forma artistica, o con ogni altro mezzo a scelta del fanciullo".

²¹ Vedi nota 17 sopra.

dà tale consenso. Pertanto, i titolari del trattamento hanno l'obbligo in conformità con la specifica menzione delle misure di trasparenza rivolta a bambini di cui all'articolo 12.1 (supportato dai considerando 38 e 58) per garantire che caso in cui riguardino i bambini o sono consapevoli che i loro beni o servizi sono particolarmente utilizzati dai bambini di un'età letterato, che le informazioni e la comunicazione devono essere convogliati in un linguaggio chiaro e semplice o in un mezzo che i bambini possono facilmente comprendere. A scanso di equivoci però, WP29 riconosce che con i bambini molto piccoli o pre-alfabetizzati, misure di trasparenza possono anche essere indirizzate a titolari della potestà genitoriale, dato che questi bambini saranno, nella maggior parte dei casi, è improbabile che capire anche i più elementari scritta o messaggi non scritte in materia di trasparenza.

16. Allo stesso modo, se un titolare del trattamento è consapevole del fatto che i loro beni / servizi sono avvalsi di By (o mirati a) gli altri membri vulnerabili della società, comprese le persone con disabilità o persone che possono avere informazioni difficoltà accesso, dovrebbero essere prese le vulnerabilità dei soggetti tali dati in considerazione dal titolare del trattamento nella sua valutazione di **come garantire la conformità con i suoi obblighi di trasparenza in relazione a tali persone interessate.**²² Ciò si riferisce alla necessità di un controllore dei dati per valutare la probabile livello del suo pubblico di comprensione, come discusso in precedenza al punto 9.

“per iscritto o con altri mezzi”

17. Ai sensi dell'articolo 12.1, la posizione di default per la fornitura di informazioni, o le comunicazioni con, interessati è che **l'informazione è in forma scritta.**²³ L'articolo 12.7 prevede, inoltre, le informazioni che devono essere fornite in combinazione con le icone standard e la questione viene considerata nella sezione relativa ai tool di visualizzazione ai punti da 49 a 53). Tuttavia, il GDPR permette anche per altri, non specificati “significa” includendo mezzi elettronici da utilizzare. La posizione di WP29 per quanto riguarda i mezzi elettronici scritta è quella in cui un controllore dei dati mantiene (o opera, in tutto o in parte, attraverso) un sito web, WP29 raccomanda l'uso di normative sulla privacy strati / comunicazioni, che permettono ai visitatori del sito web per navigare a particolari aspetti della relativa informativa sulla privacy / avviso che sono di maggior interesse per loro (vedere di più su più livelli normative sulla privacy / comunicazioni **al punto 35 a 37).**²⁴ Tuttavia, la **totalità delle informazioni rivolto alle persone interessate dovrebbe anche essere a loro** disposizione in un unico luogo o di un documento completo (sia in formato digitale o cartaceo), che può essere facilmente accessibili da un soggetto di dati, se lo desiderano consultare la totalità delle informazioni loro rivolte. È importante sottolineare che l'uso di un approccio stratificato non si limita solo a mezzi elettronici scritti per fornire informazioni alle persone. Come discusso ai punti 35 a 36 e 38 di seguito, un approccio multilivello alla fornitura di informazioni alle persone **può anche essere utilizzato impiegando una combinazione di metodi garantire trasparenza in relazione al trattamento.**

²² Per esempio, la Convenzione delle Nazioni Unite sui diritti delle persone con disabilità richiede che appropriate forme di assistenza e di sostegno sono forniti alle persone con disabilità per garantire il loro accesso alle informazioni.

²³ Articolo 12.1 si riferisce al “linguaggio” e afferma che le informazioni devono essere fornite per iscritto o con altri mezzi, compreso, se del caso, per via elettronica.

²⁴ Il riconoscimento da parte del WP29 dei vantaggi di comunicazioni a strati è già stato osservato nel parere 10/2004 sulla più armonizzato informazioni Accantonamenti e Parere 02/2013 su applicazioni su dispositivi intelligenti.

18. Naturalmente, l'uso di strati normative sulla privacy / comunicazioni digitali non è il via elettronica solo scritte che possono essere implementate dai controllori. Altri mezzi elettronici comprendono "just-in-time" le comunicazioni contestuali pop-up, tocco 3D o avvisi hover-over, e dashboard privacy. mezzi non scritte elettronici che possono essere utilizzati *Inoltre* una dichiarazione a strati privacy / avviso potrebbe includere video e smartphone o dell'Internet degli oggetti avvisi vocali.²⁵ "Altri mezzi", che non sono necessariamente elettronico, potrebbero includere, ad esempio, cartoni animati, infografica o diagrammi di flusso. Dove le informazioni sulla trasparenza diretta ai bambini, in particolare, i controllori dovrebbero considerare quali tipi di misure possono essere particolarmente accessibile ai bambini (es queste potrebbero essere fumetti / cartoni, pittogrammi, animazioni, ecc tra le altre misure).
19. È fondamentale che il metodo (s) scelto per fornire l'informazione è / sono adeguata alle circostanze particolari, cioè il modo in cui titolare e interessato interagire o il modo in cui le informazioni della persona interessata vengono raccolti. Ad esempio, fornendo solo le informazioni in forma scritta elettronica, come ad esempio in una dichiarazione privacy online / avviso potrebbe non essere adatto / praticabile in cui un dispositivo che cattura i dati personali non ha uno schermo (per esempio dispositivi internet degli oggetti / dispositivi intelligenti) per accedere al sito web / visualizzazione di tali informazioni scritte. In tali casi, **alternativo adeguato *addizionale* mezzi dovrebbero essere prese in considerazione**, ad esempio, fornendo l'informativa sulla privacy / Avviso nel manuale di istruzioni cartaceo o fornendo l'indirizzo URL del sito web (cioè la pagina specifica sul sito web) in cui la privacy online dichiarazione / notifica può essere trovato nelle istruzioni cartaceo o nella confezione. Audio (orale) la consegna delle informazioni potrebbe anche essere ulteriormente fornito se il dispositivo screenless dotato di funzionalità audio. WP29 ha già formulato raccomandazioni di tutto la **trasparenza e la fornitura di informazioni alle persone interessate a suo parere lo Sviluppo recenti nel Internet delle cose**²⁶ (come ad esempio l'uso di codici QR stampati su internet degli oggetti cose, in modo che quando scansione, il codice QR visualizzerà le informazioni di trasparenza richiesto). Queste raccomandazioni restano applicabili sotto il GDPR.

"...il informazioni possono essere fornite oralmente"

20. Articolo 12.1 prevede espressamente che le informazioni possono essere fornite oralmente ad un soggetto di dati su richiesta, a condizione che la loro identità è provata con altri mezzi. In altre parole, i mezzi impiegati devono essere più affidamento su una semplice affermazione dell'individuo che sono una determinata persona chiamata ei mezzi devono consentire al controllore per verificare l'identità di un soggetto con dati sufficienti garanzie. L'obbligo di verificare l'identità della persona prima di fornire informazioni verbalmente si applica solo alle informazioni relative all'esercizio da un dato oggetto specifico dei propri diritti ai sensi degli articoli da 15 a 22 e 34. Questo presupposto per la fornitura di informazioni per via orale non può essere applicata al fornitura di **informazioni di carattere generale privacy come indicato agli articoli 13 e 14, *futuro* gli utenti / clienti (la cui identità un responsabile del trattamento non sarebbero in grado di verificare)**. Quindi, le informazioni da fornire ai

²⁵ Questi esempi di strumenti elettronici sono solo indicativi e titolari del trattamento possono sviluppare nuovi metodi innovativi per conformarsi alle disposizioni dell'articolo 12.

²⁶ WP29 Parere 8/2014 adottata il 16 settembre 2014

Gli articoli 13 e 14 possono essere fornite mediante orale senza il controller che richiede l'identità di una persona interessata da dimostrare.

21. La fornitura orale di informazioni richieste agli articoli 13 e 14 non significa necessariamente informazioni orali fornite su base da persona a persona (cioè in persona o per telefono). Automated informazioni orali possono essere fornite in aggiunta ai mezzi scritti. Ad esempio, ciò può applicarsi nel contesto delle persone ipovedenti quando interagiscono con i fornitori di servizi della società dell'informazione, o nel contesto di dispositivi intelligenti senza griglia, come indicato al precedente punto 19. Se una titolare ha scelto di fornire informazioni un soggetto di dati per via orale, o di un soggetto di dati richiede la fornitura di informazioni per via orale o di comunicazione, la posizione di WP29 è che il titolare del trattamento dovrebbe consentire alla persona interessata di ri-ascoltare i messaggi pre-registrati. Questo è indispensabile in cui la richiesta di informazioni per via orale si riferisce alle persone con problemi di vista o di altri soggetti di dati che possono avere difficoltà ad accedere o comprendere le informazioni in forma scritta. Il titolare deve anche assicurare che esso ha un record di, e può dimostrare (ai fini del rispetto del requisito responsabilità): (i) la richiesta di informazioni per via orale, (ii) il metodo con cui la persona dell'identità è stata verificata (se del caso - vedi supra al punto

20) e (iii) il fatto che l'informazione è stata fornita alla persona.

"Gratuito"

22. Ai sensi dell'articolo 12.5,²⁷ i titolari del trattamento non possono generalmente pagare persone interessate per la fornitura di informazioni ai sensi degli articoli 13 e 14, o per le comunicazioni e le azioni intraprese ai sensi degli articoli 15-22 (sui diritti **delle persone interessate**) e l'articolo 34 (comunicazione delle violazioni di dati personali degli interessati) .²⁸ Questo aspetto della trasparenza significa anche che ogni informazione fornita sotto gli obblighi di trasparenza non può essere subordinato transazioni finanziarie, ad esempio, il pagamento per, o l'acquisto di, servizi o beni.²⁹

Informazioni da fornire alla persona interessata - articoli 13 e 14

Soddisfare

23. Il GDPR elenca le categorie di informazioni che devono essere fornite a un soggetto di dati in relazione al trattamento dei loro dati personali dove viene raccolta dalla persona interessata (articolo 13) o ottenuti da un'altra fonte (articolo 14). **Il tabella di cui all'allegato a questi**

²⁷ Questo afferma che "Le informazioni fornite ai sensi degli articoli 13 e 14 e ogni comunicazione e qualsiasi azione intrapresa ai sensi degli articoli da 15 a 22 e deve essere fornito gratuitamente 34".

²⁸ Tuttavia, ai sensi dell'articolo 12.5 del controller può addebitare un costo ragionevole in cui, ad esempio, una richiesta da parte di un soggetto dei dati in relazione alle informazioni ai sensi dell'articolo 13 e 14 o i diritti di cui agli articoli 15 - 22 o dell'articolo 34 è eccessiva o manifestamente infondata. (A parte, in relazione al diritto di accesso ai sensi dell'articolo 15.3 un controller può addebitare un costo ragionevole sulla base dei costi amministrativi per ogni ulteriore copia dei dati personali che vengono richieste da un soggetto di dati).

²⁹ A titolo di esempio, se i dati personali di un soggetto dati vengono raccolti in relazione a un acquisto, le informazioni che è necessario da fornire ai sensi dell'articolo 13, dovrebbe essere fornita prima del pagamento in corso e in corrispondenza del punto in cui vengono raccolti i dati , piuttosto che dopo che la transazione è stata conclusa. Allo stesso modo, però, in cui servizi gratuiti sono forniti alla persona interessata, le informazioni l'articolo 13 deve essere fornita prima, piuttosto che dopo, segno-in su, dato che l'articolo 13.1 richiede la fornitura delle informazioni "nel momento in cui i dati personali sono ottenuto".

linee guida riassume le categorie di informazioni che devono essere fornite ai sensi degli articoli 13 e 14. Si considera anche la natura, la portata e il contenuto di tali requisiti. Per chiarezza, la posizione di WP29 è che non c'è differenza tra lo stato delle informazioni da fornire ai sensi del sub-articolo 1 e 2 degli articoli 13 e 14 rispettivamente. Tutte le informazioni in questi sub-articoli è di uguale importanza e devono essere fornite alla persona interessata.

“misure appropriate”

24. Così come il contenuto, la forma e il modo in cui le informazioni richieste ai sensi degli articoli 13 e 14 dovrebbero essere fornite alla persona è importante. L'avviso contenente tali informazioni è spesso indicato come un avviso di protezione dei dati, l'informativa sulla privacy, sulla privacy, sulla privacy o l'avviso trattamento leale. Il GDPR non prescrive il formato o modalità con cui tali informazioni dovrebbero essere fornite alla persona interessata, ma non mettere in chiaro che è responsabilità del trattamento di adottare “misure appropriate” in relazione alla fornitura delle informazioni richieste a fini di trasparenza. Ciò significa che il titolare dovrebbe tener conto di tutte le circostanze della raccolta ed elaborazione dei dati al momento di decidere la modalità appropriata e il formato della disposizione informazioni. In particolare, dovranno essere valutate alla luce della user experience prodotto / servizio misure appropriate. Ciò significa infatti tener conto del dispositivo utilizzato (se del caso), la natura delle interfacce utente / interazioni con il titolare (l'utente “viaggio”) e le limitazioni che questi fattori comportano. Come notato sopra al punto 17, WP29 raccomanda in cui un responsabile del trattamento ha una presenza online, dovrebbe essere fornito un privacy online strati dichiarazione / preavviso.
25. Al fine di aiutare a identificare la modalità più appropriata per fornire le informazioni, in anticipo di “andare in diretta”, i titolari del trattamento possono desiderare di prova diverse modalità per mezzo di test utente (ad esempio prove di sala, o altri test standardizzati di leggibilità o l'accessibilità) per chiedere un feedback su come accessibile, comprensibile e facile da usare la misura proposta sia per gli utenti. (Vedere anche ulteriori osservazioni precedenti su altri meccanismi per effettuare test utente al punto 9). Documentare questo approccio dovrebbe anche aiutare i titolari del trattamento con i loro obblighi di responsabilità, dimostrando come lo strumento / approccio scelto per veicolare l'informazione è la più appropriata alle circostanze.

Timing per la fornitura di informazioni

26. Articoli 13 e 14 stabiliscono le informazioni che devono essere fornite alla persona interessata nella fase di inizio del ciclo di lavorazione³⁰. L'articolo 13 si applica per lo scenario in cui i dati sono raccolti presso l'interessato. Questo include i dati personali che:

³⁰ In applicazione dei principi di correttezza e di limitazione delle finalità, l'organizzazione che raccoglie i dati personali presso la persona interessata deve sempre precisare le finalità del trattamento al momento della raccolta. Se lo scopo comprende la creazione di dati personali suggeriti, lo scopo previsto di creare e ulteriore trattamento di tali dati personali dedurre, nonché le categorie di dati dedotti trattati, deve sempre essere comunicata alla persona al momento della raccolta, o prima l'ulteriore elaborazione per un nuovo scopo ai sensi dell'articolo 13.3 o dell'articolo 14.4.

- L'interessato fornisce consapevolmente a un controller di dati (ad esempio al momento di compilare un modulo online); o
- un controllore di dati raccoglie dati da un soggetto per osservazione (ad esempio utilizzando dati automatizzati acquisizione dati o dei dispositivi di cattura software quali fotocamere, apparecchiature di rete, monitoraggio Wi-Fi, RFID o altri tipi di sensori).

L'articolo 14 si applica nello scenario in cui i dati non sono stati ottenuti dalla persona interessata. Sono inclusi i dati personali che un controllore dati sono ottenuti da fonti quali:

- controllori di dati di terze parti;
- fonti disponibili al pubblico;
- broker di dati; o
- altre persone interessate.

27. Per quanto riguarda la tempistica della fornitura di tali informazioni, che fornisce in modo tempestivo è un elemento vitale degli obblighi di trasparenza e l'obbligo di elaborare i dati in modo equo. L'applicazione dell'articolo 13, ai sensi dell'articolo 13.1 devono essere fornite le informazioni *"Nel momento in cui i dati personali sono ottenuti"*. Nel caso di dati personali indirettamente ottenuti ai sensi dell'articolo 14, i tempi entro cui queste informazioni devono essere fornite alla persona interessata figurano all'articolo 14.3 (a) a (c) come segue:

- Il requisito generale è che le informazioni devono essere fornite entro un "termine ragionevole" dopo aver ottenuto i dati personali e non più tardi di un mese, *"Tenuto conto delle specifiche circostanze in cui i dati personali sono trattati"* (Articolo 14.3 (a)).
- Il limite di tempo di un mese generale di cui all'articolo 14.3 (a) può essere ulteriormente ridotta ai sensi dell'articolo 14.3 (b),³¹ che prevede una situazione in cui vengono utilizzati i dati per la comunicazione con la persona. In tal caso, l'informazione deve essere fornita al più tardi al momento della prima comunicazione con la persona interessata. Se la prima comunicazione avviene prima del termine di un mese, dopo aver ottenuto i dati personali, le informazioni devono essere fornite *al più tardi* al momento della prima comunicazione con la persona che nonostante un mese dalla punto di ottenere i dati non è scaduto. Se la prima comunicazione con un soggetto di dati si verifica più di un mese dopo aver ottenuto i dati personali, allora l'articolo

14.3 (a) continua ad applicarsi, in modo che l'informazione l'articolo 14 deve essere fornita alle persone interessate, al più tardi entro un mese dopo che è stato ottenuto.

³¹ L'uso delle parole *"Se i dati personali sono da utilizzare per..."* all'articolo 14.3 (b) indica una specifica alla posizione generale per quanto riguarda il limite massimo fissato all'articolo 14.3 (a), ma non lo sostituisce.

- Il limite di tempo di un mese generale di cui all'articolo 14.3 (a) può anche essere ridotta, ai sensi dell'art

14.3 (c) ³² che prevede una situazione in cui i dati vengono comunicati a un altro destinatario (se un terzo o meno) ³³. In tal caso, l'informazione deve essere fornita al più tardi al momento della prima rilevazione. In questo scenario, se la divulgazione avviene prima del termine di un mese, poi le informazioni devono essere fornite *al più tardi* al momento di quella prima divulgazione, nonostante il fatto che un mese dalla punto di ottenere i dati non è scaduto. Simile alla posizione con l'articolo 14.3 (b), se la divulgazione dei dati personali si verifica più di un mese dopo aver ottenuto i dati personali, l'articolo 14.3 (a), continua ancora ad applicare, in modo che l'informazione l'articolo 14 deve essere fornita al l'interessato, al più tardi entro un mese dopo che è stato ottenuto.

28. Pertanto, in ogni caso, il limite di tempo massimo entro il quale deve essere fornita l'articolo 14, le informazioni a un soggetto di dati è di un mese. Tuttavia, i principi di equità e di responsabilità sotto il GDPR richiedono i titolari del trattamento da considerare sempre le ragionevoli aspettative delle persone interessate, l'effetto che il trattamento possa avere su di loro e la loro capacità di esercitare i loro diritti in relazione a tale trattamento, al momento di decidere a quale puntare a fornire le informazioni dell'articolo 14. Responsabilità richiede controller per dimostrare la logica per la loro decisione e giustificare il motivo per cui l'informazione è stata fornita al momento è stato. In pratica, può essere difficile per soddisfare tali requisiti nel fornire informazioni al 'all'ultimo momento'. A questo proposito, il considerando 39 stabilisce, tra l'altro, che gli interessati dovrebbero essere *"Reso consapevoli dei rischi, le regole, tutele e diritti in relazione al trattamento dei dati personali e il modo di esercitare i loro diritti in relazione a tale trattamento"*. Considerando 60 si riferisce anche alla condizione che la persona è informato della esistenza del trattamento e delle sue finalità nell'ambito dei principi di trattamento equo e trasparente. Per tutte queste ragioni, la posizione di WP29 è che, per quanto possibile, i titolari del trattamento devono, in conformità con il principio di equità, fornire le informazioni agli interessati con largo anticipo dei termini stabiliti. Altre considerazioni sulla adeguatezza della tempistica tra notifica interessati delle operazioni di trattamento e di tali operazioni di trattamento effettivamente assumono effetto sono indicati paragrafi da 30 a 31 e 48.

Modifiche all'articolo 13 e all'articolo 14, le informazioni

29. Essere responsabile per quanto riguarda la trasparenza si applica non solo al momento della raccolta dei dati personali, ma tutto il ciclo di vita lavorazione, indipendentemente dal informazioni o comunicazioni veicolate. Questo è il caso, ad esempio, quando si cambia il contenuto delle normative sulla privacy / comunicazioni esistenti. Il controller dovrebbe aderire agli stessi principi quando si comunica sia l'iniziale dichiarazione sulla privacy / preavviso e eventuali successive modifiche sostanziali o sostanziali a questa affermazione / avviso. I fattori che i controllori devono considerare nel valutare ciò che è un cambiamento sostanziale o materiale comprendono l'impatto sulle persone interessate (compresa la loro capacità di esercitare i loro diritti), e in che modo inaspettato / sorprendere il

³² L'uso delle parole *"Se è prevista una comunicazione a antere destinatario ..."* all'articolo 14.3 (c) indica anche una specifica per la posizione generale per quanto riguarda il limite massimo fissato all'articolo 14.3 (a), ma non lo sostituisce.

³³ Articolo 4.9 definisce "destinatario" e chiarisce che un destinatario a cui vengono comunicati i dati personali non deve essere una terza parte. Pertanto, un destinatario può essere un controllore di dati, controllo congiunto o processore.

cambiamento sarebbe per le persone interessate. Le modifiche a una dichiarazione sulla privacy / avviso che dovrebbe sempre essere comunicati a soggetti di dati includono, tra l'altro: un cambiamento di finalità di trasformazione; una modifica l'identità del responsabile del trattamento; o di un cambiamento di come gli interessati possono esercitare i loro diritti in relazione al trattamento. Al contrario, un esempio di modifiche a una dichiarazione sulla privacy / avviso che non sono considerati da WP29 essere sostanziale o materiale includono correzioni di errori ortografici, o difetti stilistici / grammaticali. Poiché la maggior parte i clienti o gli utenti esistenti sarà solo sguardo oltre le comunicazioni di modifiche alle normative sulla privacy / comunicazioni, il regolatore dovrebbe prendere tutte le misure necessarie per garantire che questi cambiamenti vengono comunicati in modo tale che assicura che la maggior parte dei destinatari saranno effettivamente notarli. Questo significa, per esempio, che una notifica delle modifiche dovrebbe sempre essere comunicata per mezzo di una modalità appropriata (ad esempio e-mail, lettera copia cartacea, pop-up su una pagina web o altra modalità che porterà in modo efficace le modifiche alla attenzione della persona interessata) specificamente dedicato a coloro modifiche (ad esempio non insieme con il contenuto di marketing diretto), con un tale incontro la comunicazione della Articolo 12 requisiti di essere concisa, trasparente, comprensibile, facilmente accessibile e con un linguaggio chiaro e semplice. Riferimenti nel informativa sulla privacy / comunicazione secondo la quale la persona interessata dovrebbe controllare regolarmente l'informativa sulla privacy / preavviso per modifiche o aggiornamenti sono considerati non solo insufficiente, ma anche ingiusto nel contesto dell'articolo 5.1 (a).

Timing di notifica delle modifiche all'articolo 13 e all'articolo 14, le informazioni

30. Il GDPR tace sui requisiti di temporizzazione (e più precisamente i metodi) che si applicano per le notifiche di modifiche alle informazioni che sono state precedentemente fornite ad un interessato ai sensi dell'articolo 13 o 14 (ad esclusione di un ulteriore scopo destinati alla trasformazione, in cui le informazioni caso su quel ulteriore scopo deve essere notificato prima dell'inizio di quella successiva elaborazione di cui agli artt 13.3 e 14.4 - vedi sotto, al punto 45). Tuttavia, come osservato in precedenza nel contesto dei tempi per la disposizione di cui all'articolo 14 informazioni, il titolare del trattamento deve avere di nuovo per quanto riguarda i principi di correttezza e responsabilità in termini di tutte le ragionevoli aspettative della persona, o il potenziale impatto di tali modifiche sulla persona interessata. Se la modifica delle informazioni è indicativo di un cambiamento fondamentale alla natura del trattamento (ad esempio l'allargamento delle categorie di destinatari o introduzione di trasferimenti verso un paese terzo) o cambiamenti che non può essere fondamentale in termini di operazioni di trattamento, ma che possono essere rilevanti per e impatto sulla persona, quindi che le informazioni siano fornite al dati soggetti con largo anticipo del cambiamento realmente entrata in vigore e il metodo utilizzato per portare le modifiche l'attenzione della persona interessata dovrebbe essere esplicito ed efficace. Questo per garantire la persona interessata non "perdere" il cambiamento e per consentire alla persona interessata di un lasso di tempo ragionevole per loro di (a) considerare la natura e l'impatto del cambiamento e (b) esercitare i loro diritti secondo la GDPR in relazione alla la modifica (ad esempio per ritirare il consenso o di opporsi al trattamento). poi che le informazioni dovrebbero essere fornite alla persona interessata con largo anticipo del cambiamento realmente entrata in vigore e il metodo utilizzato per portare le modifiche l'attenzione della persona interessata dovrebbe essere esplicito ed efficace. Questo per garantire la persona interessata non "perdere" il cambiamento e per consentire alla persona interessata di un lasso di tempo ragionevole per loro di (a) considerare la natura e l'impatto del cambiamento e (b) esercitare i loro diritti secondo la GDPR in relazione alla la modifica (ad esempio per ritirare il consenso o di opporsi al trattamento). poi che le informazioni dovrebbero essere fornite alla persona interessata con largo anticipo del cambiamento
31. I responsabili del trattamento devono considerare attentamente le circostanze e il contesto di ogni situazione in cui è richiesto un aggiornamento di informazioni sulla trasparenza, compreso il potenziale impatto delle modifiche sui dati soggetto e la modalità utilizzata per comunicare le modifiche, ed essere in grado di dimostrare come il lasso di tempo tra il comunicazione delle modifiche e la

cambiare prendendo effetto soddisfa il principio di equità alla persona. Inoltre, la posizione di WP29 è che, in linea con il principio di equità, momento di notificare tali modifiche a persone interessate, un controllore dei dati dovrebbe anche spiegare quale sarà il probabile impatto di tali cambiamenti sulla interessati. Tuttavia, il rispetto dei requisiti di trasparenza non “whitewash” una situazione in cui le modifiche al trattamento sono così significativi che il trattamento diventa di natura completamente diversa da quello che era prima. WP29 sottolinea che tutte le altre regole del GDPR, comprese quelle relative alle ulteriori lavorazioni incompatibili, continuano ad applicarsi a prescindere dal rispetto degli obblighi di trasparenza.

32. Inoltre, anche quando l'informazione di trasparenza (ad esempio, contenuta in una dichiarazione sulla privacy / comunicazione) non materialmente cambiare, è probabile che i soggetti che hanno utilizzato il servizio per un periodo di tempo significativo, non ricorderanno le informazioni fornite a loro, in via preliminare ai sensi degli articoli 13 e / o 14. WP29 raccomanda che i controllori di facilitare agli interessati di avere continuare un facile accesso alle informazioni da essi stessi ri-conoscere con lo scopo del trattamento dei dati. In conformità con il principio di responsabilità, i controllori dovrebbero anche considerare se, ea quali intervalli, è opportuno per loro di fornire i ricordi espressi a soggetti di dati per quanto riguarda il fatto della dichiarazione sulla privacy / preavviso e dove si possono trovare.

Modalità - Formato di fornitura di informazioni

33. Entrambi gli articoli 13 e 14 si riferiscono alla obbligo per il titolare del trattamento per *“Fornire al soggetto di dati con tutte le seguenti informazioni ...”* La parola chiave qui è “fornire”. Ciò significa che il titolare del trattamento deve attivarsi per fornire le informazioni in questione alla persona o di dirigere attivamente la persona interessata alla posizione di esso (ad esempio mediante un collegamento diretto, l'uso di un codice QR, etc.) . L'interessato non deve avere a cercare attivamente informazioni coperte da questi articoli tra le altre informazioni, come ad esempio i termini e condizioni di utilizzo di un sito web o un'applicazione. L'esempio a paragrafo 11 illustra questo punto. Come notato sopra al punto 17, WP29 raccomanda che la totalità delle informazioni indirizzata agli interessati dovrebbero essere a loro disposizione in un unico luogo o un documento completo (per esempio se in forma digitale su un sito web o in formato cartaceo) che può siano facilmente accessibili dovrebbero desiderare di consultare l'insieme delle informazioni.
34. C'è una tensione inerente al GDPR tra i requisiti da un lato a fornire informazioni complete alle persone che si rendono necessarie sotto il GDPR, e dall'altro farlo in una forma che è concisa, trasparente, comprensibile e facilmente accessibile . In quanto tale, e tenendo conto dei principi fondamentali di responsabilità e correttezza, i controllori devono condurre le proprie analisi della natura, le circostanze, la portata e il contesto del trattamento dei dati personali che svolgono e decidono, entro i requisiti di legge della GDPR e tenendo conto delle raccomandazioni in questi orientamenti particolare al punto 36 di seguito, come priorità informazioni che devono essere fornite agli interessati e quali sono i livelli appropriati di dettaglio e metodi per trasmettere le informazioni.

35. Nel contesto digitale, alla luce del volume di informazioni che devono essere fornite alla persona, un approccio multilivello può essere seguita da responsabili del trattamento cui essi scelgono di utilizzare una combinazione di metodi per garantire la trasparenza. WP29 raccomanda, in particolare, che le dichiarazioni a strati sulla privacy / le comunicazioni devono essere utilizzati per collegare le varie categorie di informazioni che devono essere fornite alla persona interessata, piuttosto che la visualizzazione di tutte le informazioni in un unico avviso sullo schermo, in modo da evitare le informazioni fatica . Layered normative sulla privacy / comunicazioni possono contribuire a risolvere la tensione tra completezza e comprensione, in particolare consentendo agli utenti di navigare direttamente alla sezione della dichiarazione / avviso che desiderano leggere. Va notato che le pagine normative sulla privacy / comunicazioni non sono semplicemente annidati stratificati che richiedono parecchi scatti per raggiungere le informazioni pertinenti. Il design e il layout del primo strato della privacy / avviso devono essere tali che la persona ha una chiara panoramica delle informazioni a loro disposizione sul trattamento dei loro dati personali e dove / come si possono trovare che le informazioni dettagliate all'interno della strati della informativa sulla privacy / preavviso. E 'anche importante che le informazioni contenute all'interno dei diversi strati di un avviso a strati è coerente e che gli strati non forniscono informazioni contrastanti. Il design e il layout del primo strato della privacy / avviso devono essere tali che la persona ha una chiara panoramica delle informazioni a loro disposizione sul trattamento dei loro dati personali e dove / come si possono trovare che le informazioni dettagliate all'interno della strati della informativa sulla privacy / preavviso. E 'anche importante che le informazioni contenute all'interno dei diversi strati di un avviso a strati è coerente e che gli strati non forniscono informazioni contrastanti. Il design e il layout del primo strato della privacy / avviso devono essere tali che la persona ha una chiara panoramica delle informazioni a loro disposizione sul trattamento dei loro dati personali e dove / come si possono trovare che le informazioni dettagliate all'interno della strati della informativa sulla privacy / preavviso.
36. Per quanto riguarda il contenuto della prima modalità utilizzata da un controller per informare le persone in un approccio stratificato (in altre parole il modo principale in cui il controller prima impegna con un soggetto di dati), o il contenuto del primo strato di una privacy stratificata dichiarazione / notifica, WP29 raccomanda che il primo strato / modalità dovrebbe includere i dettagli delle finalità del trattamento, l'identità del regolatore e la descrizione dei diritti della persona interessata. (Inoltre queste informazioni devono essere direttamente portato a conoscenza di un soggetto dei dati al momento della raccolta dei dati personali es visualizzati come interessato compila un modulo online.) L'importanza di fornire questa informazione in anticipo esiste in particolare dal considerando
- 39.³⁴ Mentre i controllori devono essere in grado di dimostrare la responsabilità quali altre informazioni decidono di** priorità, la posizione di WP29 è che, in linea con il principio di correttezza, in aggiunta alle informazioni di cui sopra in questo paragrafo, il primo strato / modalità dovrebbe inoltre contenere informazioni sul trattamento che ha il maggior impatto sulla persona interessata e l'elaborazione che li potrebbe sorprendere. Pertanto, la persona interessata dovrebbe essere in grado di capire dalle informazioni contenute nel primo strato / modalità quali le conseguenze del trattamento in questione sarà per la persona (vedi anche sopra al punto 10).
37. In un contesto digitale, oltre a fornire una linea a strati sulla privacy / comunicazione, i titolari del trattamento possono **anche scegliere di usare *addizionale* strumenti di trasparenza (vedi ulteriori esempi considerati di seguito) che** forniscono informazioni su misura per il singolo soggetto di dati che è specifico alla posizione del singolo soggetto di dati in questione e dei beni / servizi che che interessato ha avvalendosi di. Va notato, tuttavia, che mentre WP29 raccomanda la

³⁴ Considerando 39 Stati, in base al principio di trasparenza, che "Tale principio riguarda, in particolare, le informazioni agli interessati sulla identità del responsabile e delle finalità del trattamento e ulteriori informazioni al fine di garantire un trattamento equo e trasparente nei confronti delle persone fisiche interessato e il diritto di ottenere la conferma e comunicazione di dati personali che lo riguardano che vengono trattati ".

uso di linea strati normative sulla privacy / comunicazioni, questa raccomandazione non esclude lo sviluppo e l'uso di altri metodi innovativi di conformità con i requisiti di trasparenza.

approccio stratificato in un ambiente non digitale

38.

Un approccio a più livelli per la fornitura di informazioni di trasparenza a soggetti i dati possono anche essere implementato in un / contesto non digitale collegato (cioè un ambiente reale, come l'impegno da persona toperson o comunicazioni telefoniche) in cui più modalità possono essere distribuiti dai responsabili del trattamento per facilitare la fornitura di informazioni. (Vedere anche paragrafi da 33 a 37 e 39 a 40 nel relazione a diverse modalità per fornire le informazioni.) Questo approccio non deve essere confuso con l'emissione separata di strati normative sulla privacy / comunicazioni. Qualunque sia i formati che vengono utilizzati in questo approccio a più livelli, WP29 raccomanda che il primo "livello" (in altre parole, il modo principale in cui il controller prima impegna con l'interessato) dovrebbe essere generalmente trasmettere le informazioni più importanti (di cui al precedente punto 36 sopra), vale a dire i dettagli delle finalità del trattamento, l'identità del controller e l'esistenza dei diritti della persona, insieme con informazioni sul maggiore impatto della lavorazione o trasformazione che potrebbe sorprendere la persona interessata. Ad esempio, dove il primo punto di contatto con un soggetto dati è telefonicamente, questa informazione potrebbe essere fornita durante la chiamata telefonica con la persona e potevano essere fornito con il bilanciamento delle informazioni richieste ai sensi dell'articolo 13/14 mediante inoltre, diversi mezzi, come ad esempio con l'invio di una copia della politica sulla privacy per e-mail e / o l'invio alla persona un collegamento al controller a strati sulla privacy online / preavviso. insieme alle informazioni sul maggiore impatto della lavorazione o trasformazione che potrebbe sorprendere la persona interessata. Ad esempio, dove il primo punto di contatto con un soggetto dati è telefonicamente, questa informazione potrebbe essere fornita durante la chiamata telefonica con la persona e potevano essere fornito con il bilanciamento delle informazioni richieste ai sensi dell'articolo 13/14 mediante inoltre, diversi mezzi, come ad esempio con l'invio di una copia della politica sulla privacy per e-mail e / o l'invio alla persona un collegamento al controller a strati sulla privacy online / preavviso. insieme alle informazioni sul maggiore impatto della lavorazione o trasformazione che potrebbe sorprendere la persona interessata. Ad esempio, dove il primo punto di contatto con

"Push" e le comunicazioni "pull"

39.

Un altro modo possibile di fornire informazioni sulla trasparenza è attraverso l'uso di "push" e le comunicazioni "pull". notifiche push comportano la fornitura di "just-in-time" avvisi informativi di trasparenza, mentre "pull" avvisi facilitano l'accesso alle informazioni con metodi come la gestione dei permessi, cruscotti privacy e tutorial "Ulteriori informazioni". Questi permettono per un'esperienza di trasparenza più usercentric per la persona interessata.

- **UN privacy cruscotto è un unico punto da cui gli interessati possono visualizzare 'informativa sulla privacy' e gestire le proprie preferenze sulla privacy, consentendo o impedendo loro dati vengano utilizzati in un certo modo per il servizio in questione. Ciò è particolarmente utile quando lo stesso servizio viene utilizzato da persone interessate su una varietà di dispositivi differenti in quanto dà loro accesso e controllo sui propri dati personali non importa come usano il servizio. Permettendo interessati per regolare manualmente le impostazioni di privacy tramite privacy cruscotto può anche rendere più facile per un sulla privacy / avviso da personalizzare riflettendo solo i tipi di lavorazione che si verificano per quel particolare soggetto dati. Incorporando un cruscotto privacy nell'architettura esistente di un servizio (ad esempio utilizzando lo stesso disegno e marchio come il resto del servizio) è preferibile perché si assicurano che l'accesso e l'uso di esso sarà intuitivo e può contribuire a incoraggiare gli utenti a impegnarsi con queste informazioni, nello stesso modo in cui farebbe con altri aspetti del servizio. Questo può essere un modo efficace di**

dimostrando che 'informativa sulla privacy' è una parte necessaria ed integrante di un servizio piuttosto che un lungo elenco di legalese.

- **UN appena in tempo avviso viene utilizzato per fornire specifiche 'informativa sulla privacy' in una metodologia ad hoc, come e quando è più rilevante per la persona interessata da leggere.** Questo metodo è utile per fornire informazioni in vari punti del processo di raccolta dati; aiuta a diffondere la fornitura di informazioni in pezzi facilmente digeribili e riduce la dipendenza da una dichiarazione singola privacy / avviso contenente informazioni che è difficile da capire fuori contesto. Ad esempio, se un soggetto di dati acquista un prodotto online, brevi informazioni esplicative può essere fornita in pop-up che accompagnano settori pertinenti di testo.

Altri tipi di "misure appropriate"

40. Dato il livello molto elevato di accesso a internet in Europa e il fatto che gli interessati possono andare online in qualsiasi momento, da più postazioni e dispositivi diversi, come si è detto, la posizione di WP29 è che una "misura appropriata" per fornire informazioni sulla trasparenza nel caso di titolari del trattamento che mantengono una presenza digitale / online, è quello di farlo attraverso un sistema elettronico sulla privacy / preavviso. Tuttavia, sulla base delle circostanze della raccolta ed elaborazione dei dati, un controllore dati può essere necessario in aggiunta (o in alternativa in cui il controllore dei dati non ha alcuna presenza digitale / linea) utilizzare altre modalità e formati di fornire le informazioni. Altri modi possibili per trasmettere le informazioni alla persona derivanti dalle seguenti diversi ambienti I dati personali possono includere le seguenti modalità applicabili all'ambiente rilevanti che sono elencati di seguito. Come notato in precedenza, un approccio stratificato può essere seguita da controllori dove scelgono di utilizzare una combinazione di tali metodi assicurando che le informazioni più importanti (vedi paragrafo 36 e 38) è sempre convogliata nella prima modalità utilizzata per comunicare con la persona .

- un. copia cartacea / ambiente di carta, ad esempio quando si entra in contratti per via postale : Chiarimenti scritti, volantini, informazioni in documentazione contrattuale, cartoni animati, infografica o diagrammi di flusso;
- b. ambiente Telefonica : Spiegazioni orali da una persona reale per consentire l'interazione e le domande a cui rispondere o automatica o pre-registrato le informazioni con la possibilità di ascoltare le informazioni più dettagliate;
- c. Screenless tecnologia / ambiente intelligente degli oggetti come il Wi-Fi di tracciamento di analisi : Icone, codici QR, allarmi vocali, informazioni scritte incorporate in carta istruzioni di set-up, i video incorporati nelle istruzioni set-up digitali, informazioni scritte sul dispositivo intelligente, i messaggi inviati via SMS o e-mail, i bordi visibili contenenti le informazioni, segnaletica pubblica o campagne di informazione pubblica;
- d. Persona all'ambiente persona, come rispondendo a sondaggi d'opinione, la registrazione di persona per un servizio : Spiegazioni orali o le note scritte fornite in formato cartaceo o morbido;

- e. ambiente "vita reale", con telecamere a circuito chiuso / registrazione drone : Schede visibili contenenti le informazioni, segnaletica pubblica, campagne di informazione pubblica o avvisi giornale / media.

Informazioni sul profiling e il processo decisionale automatizzato

41. Informazioni sull'esistenza di automatizzato il processo decisionale, tra cui profilazione, di cui agli articoli 22.1 e 22.4, insieme a informazioni significative merito alla logica relativa e il significativo e previste conseguenze del trattamento per la persona interessata, fa parte delle informazioni obbligatorie che deve essere fornita ad un soggetto di dati ai sensi degli articoli **13.2 (f) e 14.2 (g). WP29 ha prodotto linee guida per automatizzato individuale decisionali e profilatura³⁵ che dovrebbe** essere di cui per ulteriori indicazioni su come la trasparenza dovrebbe essere dato effetto nelle particolari circostanze di profiling. Va notato che, a parte i requisiti di trasparenza specifiche applicabili alle automatizzato il processo decisionale ai sensi degli articoli 13.2 (f) e 14.2 (g), i commenti in queste linee guida relative alla importanza di informare gli interessati in merito alle conseguenze del trattamento dei propri dati personali, e il principio generale che i soggetti non dovrebbero essere presi di sorpresa dal trattamento dei propri dati personali, ugualmente applicabili a **profilatura generale (non solo profilatura che viene catturato dall'articolo 22³⁶), come un tipo di lavorazione.**³⁷

Altre questioni - rischi, le regole e le garanzie

42. Considerando 39 della GDPR si riferisce anche alla fornitura di alcune informazioni che non è esplicitamente coperti dagli articoli 13 e l'articolo 14 (si veda il testo considerando supra al punto 28). Il riferimento a questo punto per rendere i dati sottopone consapevoli dei rischi, norme e delle garanzie in relazione al trattamento dei dati personali è collegato ad una serie di altre questioni. Questi includono le valutazioni di impatto sulla protezione dei dati (DPIAs). Come indicato **nella Guida del WP29 su DPIAs,**³⁸ **i titolari del trattamento possono considerare la pubblicazione della DPIA (o parte di esso),** come un modo di promuovere la fiducia nelle operazioni di trattamento e dimostrando trasparenza e la responsabilità, anche se tale pubblicazione non è obbligatoria. Inoltre, l'adesione a un codice di condotta (di cui all'art 40) può andare verso la dimostrazione trasparenza, come codici di comportamento possono essere elaborati allo scopo di specificare l'applicazione del GDPR per quanto riguarda: trattamento equo e trasparente; informazioni fornite al pubblico e agli interessati; e l'informazione fornita al, e la protezione dei bambini, tra le altre questioni.
43. Un'altra questione rilevante in materia di trasparenza è la protezione dei dati in base alla progettazione e per impostazione predefinita (come previsto dall'articolo 25). Questi principi richiedono i titolari del trattamento dei dati per costruire

³⁵ Orientamenti in materia di Automated individuale decisionali e Profiling ai fini del regolamento 2016/679, WP 251

³⁶ Questo vale per il processo decisionale basata esclusivamente su un trattamento automatizzato, tra cui profilazione, che produce effetti giuridici riguardanti la persona interessata, né parimenti significativo lui o lei colpisce.

³⁷ Considerando 60, che qui rileva, si afferma che "Inoltre, la persona interessata dovrebbe essere informata dell'esistenza di profili e le conseguenze di tale profiling".

³⁸ Linee guida sulla protezione dei dati di valutazione d'impatto (DPIA) e determinare se il trattamento è "suscettibile di provocare un alto rischio" ai fini del regolamento 2016/679, WP 248 Rev.1

Considerazioni di protezione nelle loro operazioni di trattamento e sistemi da zero, piuttosto che tenendo conto della protezione dei dati come un problema di conformità dell'ultimo minuto. Considerando 78 si riferisce ai responsabili del trattamento misure che soddisfano i requisiti di protezione dei dati di progettazione e di default includendo misure consistenti in trasparenza per quanto riguarda le funzioni e l'elaborazione dei dati personali di attuazione.

44. Separatamente, la questione della controllori congiunti è anche legato a rendere le persone interessate consapevoli dei rischi, le regole e le garanzie. Articolo 26.1 richiede controllori congiunti per determinare le rispettive responsabilità per rispettare gli obblighi sotto il GDPR in modo trasparente, in particolare per quanto riguarda l'esercizio, da interessati dei loro diritti e le funzioni di fornire le informazioni ai sensi degli articoli 13 e 14. Articolo 26.2 richiede che l'essenza della disposizione tra i controllori di dati devono essere resi disponibili alla persona. In altre parole, deve essere del tutto chiaro a un data un soggetto su quale titolare del trattamento lui o lei può avvicinarsi in cui intendono esercitare uno o più dei loro diritti secondo la GDPR.³⁹

Informazioni relative a ulteriori elaborazioni

45. Entrambi gli articoli 13 e l'articolo 14 contiene una disposizione⁴⁰ che richiede un controllore dati per informare l'interessato se intende elaborare ulteriormente i propri dati personali per scopi diversi da quelli per cui sono stati raccolti / ottenuti. Se è così, *"Il regolatore deve fornire la persona prima di tale ulteriore trattamento con informazioni su tale altra finalità e con le pertinenti informazioni di cui al paragrafo 2"*. Queste disposizioni specificamente dare attuazione al principio di cui all'art 5.1 (b) che i dati personali devono essere raccolti per finalità, esplicite e legittime, e il successivo trattamento in un modo che è *incompatibile* con questi scopi è vietata.⁴¹ La seconda parte dell'articolo 5.1 (b) stabilisce che l'ulteriore elaborazione per scopi di archiviazione di interesse pubblico, scopi di ricerca scientifica o storica o per fini statistici, deve, ai sensi dell'articolo 89.1, non può essere considerato incompatibile con le finalità iniziali. Qualora i dati personali vengono ulteriormente trattati per finalità *compatibile* con le finalità originali (articolo 6.4 informa questo problema⁴²),

Gli articoli 13.3 e 14.4 si applicano. I requisiti di questi articoli per informare l'interessato circa l'ulteriore elaborazione promuove la posizione nel GDPR che un soggetto di dati dovrebbe ragionevolmente aspettarsi che al momento e nel contesto della raccolta di dati personali che l'elaborazione

³⁹ Ai sensi dell'articolo 26.3, indipendentemente dalle condizioni del accordo tra i titolari del trattamento comuni ai sensi dell'articolo 26.1, l'interessato può esercitare i suoi diritti sotto il GDPR in materia di e contro ciascuno dei titolari del trattamento comuni.

⁴⁰ Alla articoli 13.3 e 14.4, che sono espressi in termini identici, a parte la parola "raccolta", che viene utilizzato all'articolo

13, e che viene sostituito con la parola "ottenuto" di cui all'articolo 14.

⁴¹ Vedere, per esempio, su questo principio, considerando 47, 50, 61, 156, 158; Gli articoli 6.4 e 89

⁴² Articolo 6.4 stabilisce, in modo non esaustivo, i fattori che devono essere presi in considerazione per accertare se trattamento per un'altra finalità è compatibile con lo scopo per cui i dati personali sono inizialmente raccolti, e cioè: il legame tra le finalità; il contesto in cui sono stati raccolti i dati personali; la natura dei dati personali (in particolare se le categorie particolari di dati personali o dati personali relativi a reati e condanne sono inclusi); le possibili conseguenze della ulteriore trasformazione destinati interessati; e l'esistenza di adeguate garanzie.

per uno scopo particolare può avere luogo.⁴³ In altre parole, l'interessato non deve essere preso alla sprovvista alla finalità del trattamento dei loro dati personali.

46. Gli articoli 13.3 e 14.4, nella misura in cui si riferiscono alla fornitura di *"Ulteriori informazioni rilevanti di cui al paragrafo 2"*, può essere interpretato a prima vista come lasciare qualche elemento di apprezzamento al titolare per la misura nonché le particolari categorie di informazioni dal rispettivo sotto-paragrafo 2 (ossia l'articolo 13.2 o 14.2 a seconda del caso) che devono essere fornite alla soggetto. (Considerando 61 si riferisce a questo come *"altre informazioni necessarie"*.) Tuttavia la posizione di default è che tutte le informazioni di cui al presente sub-articolo devono essere fornite alla persona interessata a meno che una o più categorie di informazioni non esista o non è applicabile.
47. WP29 raccomanda che, al fine di essere trasparente, equa e responsabile, i controllori dovrebbero prendere in considerazione la diffusione delle informazioni agli interessati nella loro privacy / avviso sulla analisi di compatibilità **effettuata ai sensi dell'articolo 6.4⁴⁴ dove una base giuridica diversa consenso o nazionale / UE è invocata per il nuovo scopo di elaborazione.** (In altre parole, una spiegazione di come trattamento per l'altro scopo (s) è compatibile con lo scopo originale). Questo per consentire interessati la possibilità di prendere in considerazione la compatibilità del ulteriore trattamento e le garanzie previste e decidere se esercitare i loro diritti

ad esempio il diritto di restrizione della trasformazione o il diritto di opporsi al trattamento, tra gli altri.⁴⁵ Dove controller scelgono di non includere tali informazioni in Privacy / dichiarazione, WP29 raccomanda che rendono chiaro agli interessati che possono ottenere le informazioni su richiesta.

48. Collegato all'esercizio dei diritti della persona interessata è la questione della tempistica. Come sottolineato in precedenza, la fornitura di informazioni in modo tempestivo è un elemento vitale dei requisiti di trasparenza di cui agli articoli 13 e 14 ed è intrinsecamente legata al concetto di trattamento leale. Informazione in relazione alla *ulteriore elaborazione* devono essere fornite *"prima di tale ulteriore trattamento"*. La posizione di WP29 è che dovrebbe verificarsi un periodo ragionevole tra la notifica e l'elaborazione inizia piuttosto che un inizio immediato al trattamento previa notifica che è ricevuto dalla persona. Questo dà interessati i vantaggi pratici del principio di trasparenza, permettendo loro una significativa opportunità di considerare (e potenzialmente esercitare i loro diritti in relazione a) l'ulteriore lavorazione. Che cosa è un ragionevole periodo dipenderà dalle circostanze particolari. Il principio di equità richiede che il più invadenti (o meno prevedibile) l'ulteriore lavorazione, più lungo è il periodo dovrebbe essere. Allo stesso modo, il principio di responsabilità richiede che i titolari siano in grado di dimostrare come le determinazioni che hanno fatto per quanto riguarda i tempi per la fornitura di tali informazioni sono giustificate nelle circostanze e in che modo la tempistica è nel complesso giusto interessati. (Vedere anche i commenti precedenti in relazione ad accertare tempi ragionevoli sopra ai punti da 30 a 32.)

⁴³ Considerando 47 e 50

⁴⁴ Inoltre si fa riferimento nel considerando 50

⁴⁵ Come riferito al considerando 63, ciò consentirà un interessato per esercitare il diritto di accesso al fine di conoscere e verificare la legittimità del trattamento.

strumenti di visualizzazione

49. È importante sottolineare che il principio di trasparenza nella GDPR non si limita ad essere effettuato semplicemente attraverso la comunicazione in lingua (scritta o orale). Il GDPR prevede strumenti di visualizzazione (riferimento in particolare, icone, meccanismi di certificazione, e le guarnizioni di protezione dei dati e marchi) se del caso. **Considerando 58⁴⁶ indica che l'accessibilità delle informazioni rivolta al pubblico o agli interessati è particolarmente importante in un ambiente online.**⁴⁷

Icone

50. Considerando 60 prevede informazioni da fornire ad un soggetto di dati "in combinazione" con icone standardizzati, consentendo così un approccio a più livelli. Tuttavia, l'uso di icone non deve sostituire semplicemente le informazioni necessarie per l'esercizio dei diritti di un soggetto di dati né devono essere utilizzato come sostituto per il rispetto degli obblighi del responsabile del trattamento ai sensi degli articoli 13 e 14. L'articolo 12.7 prevede l'uso di tali icone affermando che:

"Le informazioni che devono essere fornite agli interessati ai sensi degli articoli 13 e 14 possono essere fornite in combinazione con le icone standardizzati al fine di dare in modo facilmente visibile, comprensibile e chiaramente leggibile una panoramica significativa del trattamento previsto. Dove le icone vengono presentati elettronicamente essi devono essere leggibili a macchina".

51. Come l'articolo 12,7 afferma che *"Se le icone vengono presentate elettronicamente, essi saranno machinereadable"*, questo suggerisce che ci possono essere situazioni in cui le icone non sono presentati per via elettronica,⁴⁸ per esempio le icone sul lavoro di ufficio fisico, dispositivi internet degli oggetti o confezione del dispositivo degli oggetti, le comunicazioni in luoghi pubblici circa il monitoraggio Wi-Fi, i codici QR e le comunicazioni a circuito chiuso.
52. Chiaramente, lo scopo di utilizzare icone è quello di migliorare la trasparenza per gli interessati, riducendo potenzialmente la necessità di grandi quantità di informazioni scritte da presentare ad un soggetto di dati. Tuttavia, l'utilità di icone per trasmettere in modo efficace le informazioni richieste ai sensi degli articoli 13 e 14 ai titolari dei dati dipende dalla standardizzazione dei simboli / immagini di essere

⁴⁶ "Tali informazioni potrebbero essere fornite in formato elettronico, per esempio, quando si rivolge al pubblico, attraverso un sito web.

Questo è di particolare rilevanza in situazioni in cui la proliferazione di attori e la complessità tecnologica della pratica rendono difficile per la persona interessata a conoscere e capire se, da chi e per quale scopo i dati personali che lo riguardano o lei sono raccolti, come ad esempio nel caso della pubblicità online ".

⁴⁷ In questo contesto, i controllori devono tener conto interessati ipovedenti (ad esempio rosso-verde cecità colore).

⁴⁸ Non esiste una definizione di "machinereadable" nel GDPR ma considerando 21 della direttiva 2013/37 / EU17 definisce "machinereadable" come:

"Un formato di file strutturato in modo che le applicazioni software possono facilmente identificare, riconoscere e estrarre dati specifici, comprese le dichiarazioni individuali di fatto, e la loro struttura interna. I dati codificati in file che sono strutturati in un formato leggibile dalla macchina sono dati leggibili a macchina. formati leggibili meccanicamente possono essere aperte o di proprietà; possono essere norme formali o meno. Documenti codificati in un formato di file che limita elaborazione automatica, poiché i dati non può, o può non facilmente, di estrarre da esse, non deve essere considerato in un formato leggibile dalla macchina. Gli Stati membri dovrebbero, se del caso incoraggiare l'uso di formati aperti, a lettura ottica."

universalmente utilizzato e riconosciuto in tutta l'UE come abbreviazione di tali informazioni. A questo proposito, il GDPR assegna responsabilità per lo sviluppo di un codice di icone alla Commissione, ma in ultima analisi, il Comitato europeo per la protezione dei dati può, sia su richiesta della Commissione o di propria iniziativa, fornire alla Commissione un parere su tali icone.⁴⁹ WP29 riconosce che, in linea con il considerando 166, lo sviluppo di un codice di icone deve essere centrata su un approccio evidence-based e in anticipo di qualsiasi tale standardizzazione sarà necessario per vasta ricerca da condurre in collaborazione con l'industria e la più ampia pubblica per l'efficacia di icone in questo contesto.

meccanismi di certificazione, sigilli e segni

53. A parte l'uso di icone standardizzati, il GDPR (articolo 42) prevede anche l'utilizzo di meccanismi di certificazione di protezione dei dati, le guarnizioni di protezione dei dati e marchi al fine di dimostrare la conformità con la GDPR delle operazioni di trattamento da parte dei responsabili dei dati e processori e migliorare la trasparenza per gli interessati.⁵⁰ WP29 sarà emanare linee guida sui meccanismi di certificazione a tempo debito.

Esercizio dei diritti degli interessati

54. La trasparenza pone un triplice obbligo per i titolari del trattamento nella misura in cui i diritti delle persone interessate sotto il GDPR sono interessati, in quanto deve:⁵¹
- fornire informazioni alle persone interessate sui loro diritti⁵² (come richiesto ai sensi degli articoli 13.2 (b) e 14.2 (c));
 - rispettare il principio di trasparenza (cioè relativa alla qualità delle comunicazioni di cui all'articolo 12.1) durante la comunicazione con le persone interessate in relazione ai loro diritti ai sensi degli articoli da 15 a 22 e 34; e
 - facilitare l'esercizio dei diritti dell'interessato ai sensi degli articoli da 15 a 22.
55. I requisiti GDPR in relazione all'esercizio di questi diritti e la natura delle informazioni richieste sono progettati per *posizione per significato* interessati in modo che possano rivendicare i propri diritti e tenere i titolari del trattamento responsabili per il trattamento dei loro dati personali. Considerando 59 sottolinea che *"Modalità dovrebbero essere forniti per facilitare l'esercizio dei diritti della persona interessata"* e che il titolare dovrebbe *"Fornire anche mezzi*

⁴⁹ L'articolo 12.8 prevede che la Commissione ha il potere di adottare atti delegati ai sensi dell'articolo 92 ai fini della determinazione delle informazioni da presentare da parte delle icone e le informazioni per la fornitura di icone standardizzati. Considerando 166 (che si occupa di atti delegati della Commissione in generale) è istruttivo, a condizione che la Commissione deve svolgere consultazioni adeguate durante i lavori preparatori, anche a livello di esperti. Tuttavia, il Comitato europeo per la protezione dei dati (EDPB) ha anche un importante ruolo consultivo da svolgere in relazione alla standardizzazione delle icone come l'articolo 70.1 (r) stabilisce che l'EDPB, di propria iniziativa o, se del caso, su richiesta della Commissione, fornire alla Commissione un parere sulle icone.

⁵⁰ Vedere il riferimento al considerando 100

⁵¹ Nella sezione Trasparenza e modalità delle GDPR sui dati diritti soggetti (sezione 1, capitolo III, ossia l'articolo

12)

⁵² Accesso, rettifica, cancellazione, la limitazione lavorazione, oggetto di trattamento, portabilità

per le richieste da effettuare elettronicamente, in particolare quando i dati personali sono trattati per via elettronica". La modalità fornita da un regolatore di dati per gli interessati l'esercizio dei diritti deve essere adeguata al contesto e la natura del rapporto e le interazioni tra il controllore e l'interessato. A tal fine, un responsabile del trattamento potrebbe desiderare di fornire uno o più diverse modalità per l'esercizio dei diritti che sono riflettenti dei diversi modi in cui gli interessati che interagiscono con titolare del trattamento.

Esempio

Un fornitore di servizi di salute utilizza un modulo elettronico sul suo sito web, e moduli cartacei nelle recezioni delle sue cliniche, per facilitare la presentazione di richieste di accesso per i dati personali sia online che di persona. Mentre fornisce queste modalità, il servizio sanitario ancora accetta le richieste di accesso presentate in altri modi (ad esempio per lettera e per e-mail) e fornisce un punto dedicato di contatto (cui si può accedere per email e per telefono) per aiutare i soggetti di dati con il esercizio dei loro diritti.

Eccezioni all'obbligo di fornire informazioni

Articolo 13 eccezioni

56. L'unica eccezione dell'articolo 13 obblighi di un responsabile del trattamento in cui ha raccolto i dati personali direttamente da un soggetto di dati si verifica *"Dove e nella misura in cui, la persona interessata ha già le informazioni"*.⁵³ Il principio di responsabilità richiede che i titolari dimostrano (e documentare) quali informazioni l'interessato ha già, come e quando hanno ricevuto e che nessun cambiamento da allora sono venuto in mente che le informazioni che lo renderebbe obsoleto. Inoltre, l'uso della frase "in quanto" di cui all'articolo 13.4 rende chiaro che, anche se la persona interessata abbia precedentemente fornito con alcune categorie dall'inventario delle informazioni di cui all'articolo 13, c'è ancora l'obbligo per il titolare del trattamento di integrare tali informazioni al fine di garantire che la persona interessata ha ora una serie completa di informazioni di cui agli articoli 13.1 e 13.2. Quanto segue è un esempio di buone pratiche circa le modalità limitata in cui l'eccezione articolo 13.4 deve essere interpretata.

Esempio

Un individuo si iscrive a un servizio di posta elettronica on-line e riceve tutta l'articolo richiesto 13.1 e 13.2 le informazioni al punto di iscrizione. Sei mesi più tardi la persona attiva una funzionalità di messaggia istantanea collegata tramite il fornitore del servizio di posta elettronica e fornisce loro numero di telefono cellulare per farlo. Il fornitore di servizi offre la persona interessata certo l'articolo 13.1 e 13.2 informativa sul trattamento del numero di telefono (ad es scopi e la base giuridica per il trattamento, i destinatari, il periodo di conservazione), ma non fornisce altre informazioni che l'individuo già

⁵³ Articolo 13.4

ha da 6 mesi fa e che da allora non è cambiato (ad esempio le identità e gli estremi del titolare e il responsabile della protezione dei dati, informazioni sui dati diritti soggetti e il diritto di lamentarsi con l'autorità di vigilanza competente). Come una questione di buone prassi tuttavia, la suite completa di informazioni dovrebbero essere fornite alla persona interessata di nuovo, ma la persona interessata anche dovrebbe essere in grado di dire che cosa facilmente informazioni tra è nuovo. Il nuovo trattamento per le finalità del servizio di messaggistica istantanea può influenzare la persona in un modo che avrebbe chiesto loro di cercare di esercitare un diritto che possono avere dimenticato, essendo stata informata sei mesi prima. Fornendo tutte le informazioni aiuta ancora una volta a garantire la persona interessata rimane ben informati sulle modalità di utilizzo dei propri dati e dei loro diritti.

Articolo 14 eccezioni

57. Articolo 14 ritaglia un insieme molto più ampio di deroghe all'obbligo informazioni su un controllore dei dati in cui i dati personali non è stato ottenuto dalla persona interessata. Queste eccezioni dovrebbero, in linea di massima, essere interpretate ed applicate in modo restrittivo. Oltre alle circostanze in cui la persona interessata ha già le informazioni in questione (articolo

14.5 (a)), l'articolo 14.5 permette anche per le seguenti eccezioni:

- La fornitura di tali informazioni sia impossibile o comporta uno sforzo sproporzionato, in particolare per la lavorazione a scopi di archiviazione di interesse pubblico, scopi di ricerca scientifica o storici o fini statistici, o qualora possa rendere il raggiungimento degli obiettivi del trattamento impossibile o seriamente mettere in pericolo loro;
- Titolare del trattamento è soggetto a una legge nazionale o requisito diritto UE di ottenere o divulgare i dati personali e che la legge prevede adeguate protezioni per gli interessi legittimi della persona interessata; o
- L'obbligo del segreto professionale (tra cui un obbligo di legge di segretezza) che è regolata dal diritto nazionale o comunitario significa che i dati personali devono rimanere riservati.

Si rivela impossibile, sforzo sproporzionato e seria compromissione degli obiettivi

58. L'articolo 14.5 (b) permette per 3 situazioni distinte in cui l'obbligo di fornire le informazioni di cui agli articoli 14.1, 14.2 e 14.4 è sollevato:

- (io) Qualora risulti impossibile (in particolare per l'archiviazione, la ricerca scientifica / storica o fini statistici); (li) Qualora comporti uno sforzo sproporzionato (in particolare per l'archiviazione, la ricerca scientifica / storica o fini statistici); o (iii) Dove fornendo le informazioni richieste ai sensi dell'articolo 14.1 renderebbe il raggiungimento degli obiettivi del trattamento impossibile o seriamente mettere in pericolo loro.

59. La situazione in cui "si rivela impossibile" ai sensi dell'articolo 14.5 (b) fornire le informazioni è una situazione tutto o niente perché qualcosa è impossibile o non lo è; non ci sono gradi di impossibilità. Così, se un responsabile del **trattamento cerca di fare affidamento su questa esenzione deve dimostrare i fattori che in realtà *impedirlo* dal** fornire le informazioni in questione alle persone interessate. Se, dopo un certo periodo di tempo, i fattori che hanno causato la "impossibilità" non esistono più e diventa possibile fornire le informazioni agli interessati, allora il titolare del trattamento deve immediatamente farlo. In pratica, ci saranno molto poche situazioni in cui un controllore dei dati può dimostrare che in realtà è impossibile fornire le informazioni alle persone. L'esempio seguente dimostra questo.

Esempio

L'interessato si registra per un servizio di abbonamento online post-pagato. Dopo la registrazione, il titolare del trattamento raccoglie i dati di credito da un'agenzia di credito di segnalazione sui dati soggetti al fine di decidere se fornire il servizio. Il protocollo del controllore è quello di informare gli interessati della raccolta di questi dati di credito entro tre giorni dalla raccolta, ai sensi dell'articolo 14.3 (a). Tuttavia, l'indirizzo della persona interessata e il numero di telefono non è registrato nei registri pubblici (la persona è in realtà che vivono all'estero). L'interessato non ha lasciato un indirizzo email al momento della registrazione per il servizio o l'indirizzo e-mail non è valido. Il controllore rileva che non ha mezzi per contattare direttamente l'interessato. In questo caso, tuttavia, il controllore può dare informazioni sulla raccolta dei dati di segnalazione di credito sul suo sito web, prima della registrazione.

Impossibilità di fornire la fonte dei dati

60. Il considerando 61 afferma che " *in cui l'origine dei dati personali non può essere fornito alle persone interessate, perché sono state utilizzate diverse fonti, dovrebbero essere fornite informazioni di carattere generale* ". Il sollevamento del requisito di fornire informazioni sulla fonte dei dati personali si applica solo quando questo non è possibile perché diversi pezzi di dati personali relativi allo stesso oggetto dati non possono essere attribuiti ad una particolare sorgente. Ad esempio, il solo fatto che un database comprendente i dati personali di soggetti multipli di dati è stato compilato da un controllore dati utilizzando più di una sorgente non è sufficiente a sollevare tale richiesta se è possibile (anche se in termini di tempo o oneroso) per identificare il fonte da cui i dati personali delle persone interessate singoli **derivati**. **Dati i requisiti di protezione dei dati in base alla progettazione e per impostazione predefinita,**⁵⁴ **meccanismi di** trasparenza dovrebbero essere integrati in sistemi di elaborazione da zero in modo che tutte le fonti di dati personali ricevuti in un'organizzazione possono essere monitorati e risalire alla loro fonte in qualsiasi punto del ciclo di vita di elaborazione dati (vedi sopra punto 43).

⁵⁴ Articolo 25

“Sforzo sproporzionato”

61. Ai sensi dell'articolo 14.5 (b), come con il “si rivela impossibile” situazione “sforzo sproporzionato” può applicare anche, in particolare, per l'elaborazione *“Per l'archiviazione di interesse pubblico, scopi di ricerca scientifica o storici o fini statistici, fatte salve le garanzie di cui all'articolo 89 (1)”*. Considerando 62 fa riferimento anche questi obiettivi come i casi in cui la fornitura di informazioni alla persona interessata comporterebbe uno sforzo sproporzionato e afferma che a questo proposito, il numero delle persone interessate, l'età dei dati e delle eventuali garanzie appropriate adottate dovrebbe essere preso in considerazione. Data l'enfasi nel considerando 62 e l'articolo 14.5 (b) l'archiviazione, la ricerca e l'elaborazione di statistiche per quanto riguarda l'applicazione di tale esenzione, la posizione di WP29 è che questa eccezione non dovrebbe essere

di routine invocata dai responsabili del trattamento che non sono trattamento dei dati personali ai fini di archiviazione nel pubblico interesse, per scopi di ricerca scientifica o storica o scopi statistici. WP29 sottolinea il fatto che quando questi sono gli scopi perseguiti, le condizioni di cui all'articolo 89.1 devono ancora essere rispettate e la fornitura delle informazioni deve costituire uno sforzo sproporzionato.

62. Nel determinare quale costituisce sia impossibilità o eccessiva sensi dell'articolo 14.5 (b), è importante che non vi siano eccezioni comparabili ai sensi dell'articolo 13 (in cui i dati personali vengono raccolti da un interessato). L'unica differenza tra un articolo 13 e l'articolo 14, una situazione è che in quest'ultimo, i dati personali non sono raccolti presso l'interessato. Ne consegue che impossibilità o eccessiva si manifesta tipicamente in virtù di circostanze che non applicano se i dati personali sono raccolti presso la persona. In altre parole, l'impossibilità o eccessiva devono essere collegati direttamente al fatto che i dati sono stati ottenuti diversi da quelli della persona.

Esempio

Un grande ospedale metropolitano richiede tutti i pazienti per le procedure di giorno, ricoveri a lungo termine e gli appuntamenti di compilare un Modulo informazioni paziente che cerca i dettagli di due (interessati) next-of-kin. Dato il grande volume di pazienti che passano attraverso l'ospedale su base giornaliera, che comporta uno sforzo sproporzionato da parte dell'ospedale per dare a tutti coloro che sono stati elencati come next-of-kin sulle forme compilati dai pazienti ogni giorno con le informazioni richieste ai sensi dell'articolo 14.

63. I fattori di cui sopra nel considerando 62 (numero di persone interessate, l'età dei dati e gli eventuali garanzie appropriate adottate) può essere indicativo dei tipi di problemi che contribuiscono a un controller di dati avente utilizzare sforzo sproporzionato per notificare un interessato di l'informazioni pertinenti dell'articolo 14.

Esempio

ricercatori storici che cercano di rintracciare lignaggio sulla base di cognomi ottenere indirettamente un grande insieme di dati relativi a 20.000 persone interessate. Tuttavia, il set di dati è stato raccolto 50

anni fa, non è stato aggiornato da allora, e non contiene informazioni di contatto. Data la dimensione del database e più in particolare, l'età dei dati, comporta uno sforzo sproporzionato per i ricercatori per cercare di rintracciare le persone interessate individualmente al fine di fornire loro l'articolo 14, le informazioni.

64. Quando un responsabile del trattamento cerca di invocare la deroga di cui all'articolo 14.5 (b) in base a tale disposizione delle informazioni comporterebbe uno sforzo sproporzionato, si dovrebbe effettuare un esercizio di bilanciamento per valutare lo sforzo richiesto per il controller di dati per fornire le informazioni alla persona contro l'impatto e gli effetti sulla persona se lui o lei non è stato fornito con le informazioni. Questa valutazione deve essere documentata dal titolare del trattamento in conformità con i suoi obblighi di rendicontazione. In tal caso, l'articolo 14.5 (b) specifica che il controllore deve prendere misure appropriate per proteggere diritti, le libertà della persona interessata e interessi legittimi. Ciò vale anche quando un controllore determina che la fornitura dell'informazione si riveli impossibile, o sarebbe probabilmente renda impossibile o gravemente il raggiungimento degli obiettivi del trattamento. Una misura adeguata, di cui all'articolo 14.5 (b), che i controllori devono sempre prendere è quello di rendere le informazioni disponibili al pubblico. Un controllore può fare questo in un certo numero di modi, per esempio mettendo le informazioni sul suo sito web, o da una pubblicità in modo proattivo le informazioni in un giornale o sui manifesti nei suoi locali. Altre misure appropriate, oltre a rendere le informazioni disponibili al pubblico, dipenderà dalle circostanze del trattamento, ma possono includere: intraprendere una valutazione d'impatto sulla protezione dei dati; applicando tecniche pseudonimizzazione ai dati; minimizzando i dati raccolti e il periodo di conservazione; e l'attuazione di misure tecniche e organizzative per garantire un elevato livello di sicurezza. Inoltre, vi possono essere casi in cui un controllore dei dati elabora i dati personali che non richiede l'identificazione di un soggetto di dati (per esempio dati pseudonimizzati). In questi casi, l'articolo 11.1 può anche essere rilevante in quanto si afferma che un responsabile del trattamento non è tenuto a mantenere, acquisire o elaborare le informazioni aggiuntive al fine di individuare il soggetto dei dati ai soli fini del rispetto del GDPR.

compromissione grave degli obiettivi

65. La situazione finale di cui all'articolo 14.5 (b) è dove la fornitura di informazioni a un soggetto di dati ai sensi dell'articolo 14.1 del titolare del trattamento è idonea a rendere impossibile o gravemente il raggiungimento degli obiettivi di elaborazione. Per fare affidamento su questa eccezione, i titolari del trattamento devono dimostrare che la fornitura delle informazioni di cui all'articolo 14.1 annullerebbe gli obiettivi del trattamento. In particolare, il ricorso a questo aspetto dell'articolo 14.5 (b) presuppone che il trattamento dei dati soddisfa tutti i principi di cui all'articolo 5 e che, soprattutto, in tutte le circostanze, il trattamento dei dati personali è giusto e che ha una base giuridica.

Esempio

Bank A è soggetta a un requisito obbligatorio ai sensi della legislazione antiriciclaggio segnalare attività sospette relative ai conti detenuti con esso al relativo all'autorità applicazione della legge finanziaria.
Banca A riceve informazioni da Bank B (in

un altro Stato membro) che un titolare del conto ha incaricato per trasferire denaro a un altro conto presso Banca A che appare sospetto. Bank A passa questi dati riguardanti la sua titolare del conto e le attività sospette alle autorità pertinenti l'applicazione della legge finanziaria. La legislazione antiriciclaggio in questione lo rende un reato penale per una banca riferire al "Tip off", il titolare del conto che essi possono essere soggetti a indagini normative. In questa situazione, l'articolo 14.5 (b) si applica, perché fornisce l'interessato (il titolare del conto con la Banca A) dell'articolo 14, le informazioni sul trattamento dei dati personali del titolare del conto di informazioni ricevute da Banca B seriamente mettere in pericolo gli obiettivi della legislazione, che comprende la prevenzione di "soffiate". Però,

Ottenere o divulgazione è espressamente prevista dalla legge

66. L'articolo 14.5 (c) consente un sollevamento dei requisiti di informazione di cui agli articoli 14.1, 14.2 e 14.4 nella misura in cui l'ottenimento o la divulgazione di dati personali *"È espressamente prevista dal diritto dell'Unione o degli Stati membri a cui è soggetto il responsabile"*. Tale esenzione è subordinata la legge in questione fornendo *"Misure appropriate per proteggere gli interessi legittimi della persona interessata"*. Tale legge deve affrontare direttamente titolare e l'ottenimento o la divulgazione in questione deve essere vincolante per il responsabile del trattamento. Di conseguenza, il controllore dei dati deve essere in grado di dimostrare come la legge in questione si applica a loro e richiede a uno ottenere o divulgare i dati personali in questione. Mentre è in Unione o la legge dello Stato membro di inquadrare la legge in modo tale che esso fornisce *" misure appropriate per proteggere gli interessi legittimi della persona interessata"*, il titolare deve garantire (ed essere in grado di dimostrare) che il suo ottenimento o la divulgazione dei dati personali conforme a tali misure. Inoltre, il controllore dei dati deve far capire alle persone che ottiene o divulga i dati personali in conformità con la legge in questione, a meno che non ci sia un divieto legale impedendo il titolare di farlo. Ciò è in linea con il considerando 41 della GDPR, in cui si afferma che una legge o un provvedimento legislativo dovrebbe essere chiara e precisa, e la sua applicazione deve essere prevedibile per persone soggette ad essa, conformemente alla giurisprudenza della Corte di giustizia l'Unione europea e la Corte europea dei diritti dell'uomo. Tuttavia, l'articolo 14.5 (c) non si applica quando il titolare del trattamento è l'obbligo di **ottenere dati direttamente da un interessato, nel qual caso si applicherà l'articolo 13**. In tal caso, l'unica deroga sotto il GDPR dispensa il controllore di fornire agli interessati le informazioni sul trattamento sarà che l'articolo 13.4 (cioè dove e nella misura in cui la persona ha già le informazioni). Tuttavia, come indicato di seguito al punto 68, a livello nazionale, gli Stati membri possono anche legiferare, ai sensi dell'articolo 23, per le restrizioni più specifiche al diritto di trasparenza di cui all'articolo 12 e alle informazioni ai sensi degli articoli 13 e 14.

Esempio

Un'autorità fiscale è soggetta ad un requisito obbligatorio ai sensi del diritto nazionale, per ottenere i dettagli di stipendi dei dipendenti dai loro datori di lavoro. I dati personali non è ottenuta

dalle persone interessate e, pertanto, l'autorità fiscale è soggetta alle disposizioni di cui all'articolo 14. Come l'ottenimento dei dati personali da parte dell'amministrazione fiscale dai datori di lavoro è espressamente previsto dalla legge, gli obblighi di informazione di cui all'articolo 14 non si applicano all'imposta l'autorità in questo caso.

Riservatezza in virtù di un obbligo segretezza

67. L'articolo 14.5 (d), prevede un'esenzione al requisito informazioni su titolari del trattamento cui i dati personali *“Deve rimanere soggetta riservata ad un obbligo di segreto professionale regolamentata dal diritto dell'Unione o degli Stati membri, tra cui l'obbligo legale di segretezza”*. Se un controllore dei dati intende avvalersi di questa esenzione, deve essere in grado di dimostrare di aver adeguatamente identificato un tale esenzione e di mostrare come l'obbligo del segreto professionale si rivolge direttamente al titolare del trattamento in modo tale che vieta il titolare del trattamento di fornire tutte le informazioni di cui agli articoli 14.1, 14.2 e 14.4 per la persona interessata.

Esempio

Un medico (titolare del trattamento) ha l'obbligo professionale di segretezza in relazione alle informazioni mediche dei suoi pazienti. Un paziente (nei cui confronti si applichi l'obbligo del segreto professionale) fornisce il medico con informazioni sul suo stato di salute, relativa ad una condizione genetica, che un certo numero di suoi parenti stretti hanno anche. Il paziente fornisce anche il medico con alcuni dati personali dei suoi parenti (delle persone interessate) che hanno la stessa condizione. Il medico non è tenuto a fornire quei parenti con l'articolo 14 informazioni come la deroga di cui all'articolo

14.5 (d) si applica. Se il medico dovesse fornire le informazioni dell'articolo 14, ai parenti, l'obbligo del segreto professionale, che si deve al suo paziente, sarebbe stata violata.

Restrizioni al diritto di dati soggetti

68. L'articolo 23 prevede che gli Stati membri (o UE) di legiferare per limitare ulteriormente la portata dei diritti della **persona in relazione alla trasparenza ei dati sostanziali diritti soggetti**⁵⁵ dove tali misure rispettare il contenuto essenziale dei diritti e delle libertà fondamentali e siano necessarie e proporzionate per tutelare uno o più dei dieci obiettivi di cui all'articolo 23.1 (a) a (j). Qualora tali misure nazionali diminuiscono sia i diritti della persona interessata o di specifici obblighi di trasparenza generale, che altrimenti si applicherebbero ai responsabili del trattamento sotto il GDPR, il titolare del trattamento dovrebbe essere in grado di dimostrare come la disposizione nazionale si applica a loro. Come sancito dall'articolo 23.2 (h), la misura legislativa deve contenere una disposizione per il diritto della persona di essere informato su una restrizione

⁵⁵ Come di cui agli articoli da 12 a 22 e 34, e all'articolo 5, nella misura in cui le sue disposizioni corrispondono ai diritti e gli obblighi di cui agli articoli da 12 a 22.

i loro diritti, a meno che sia informandoli possono pregiudicare la finalità della restrizione. Coerentemente con questo, e in linea con principio di equità, il controllore dati dovrebbe anche informare le persone che si affidano a (o si contano, nel caso di un particolare soggetto dati destra viene esercitato) tale *una restrizione legislativo nazionale* per l'esercizio dei diritti della persona, o per l'obbligo di trasparenza, a meno che ciò sarebbe pregiudizievole per lo scopo della restrizione legislativa. Come tale, la trasparenza richiede i titolari del trattamento di fornire adeguate informazioni in anticipo agli interessati circa i loro diritti e le eventuali avvertenze particolari per quei diritti che il controllore può cercare di fare affidamento su, in modo che la persona interessata non è preso di sorpresa da una restrizione presunta di un diritto particolare quando poi tentano di esercitare contro il controller. In relazione a pseudonimi e minimizzazione dei dati, e nella misura in cui i controllori di dati possono pretendere di invocare l'art 11 della GDPR, WP29 ha confermato in precedenza nel parere 3/2017⁵⁶ che l'articolo 11 del GDPR deve essere interpretato come un modo di far rispettare genuina minimizzazione dei dati senza ostacolare l'esercizio dei diritti della persona, e che l'esercizio dei diritti della persona interessata deve essere reso possibile con l'aiuto di ulteriori informazioni fornite dalla persona interessata.

69. Inoltre, l'articolo 85 impone agli Stati membri, per legge, di conciliare la protezione dei dati con il diritto alla libertà di espressione e informazione. Ciò richiede, tra l'altro, che gli Stati membri prevedano esenzioni o deroghe a talune disposizioni della GDPR (compresi dagli obblighi di trasparenza di cui agli articoli 12 - 14) adeguate per il trattamento previsto a fini di espressione giornalistica, accademici, artistici o letterari, se essi sono necessari per conciliare i due diritti.

Trasparenza e violazioni dei dati

70. WP29 ha prodotto linee guida separate violazioni dei dati⁵⁷ ma per gli scopi di queste linee guida, gli obblighi di un responsabile del trattamento in relazione alla comunicazione delle violazioni di dati ad un soggetto di dati devono tenere pienamente conto delle esigenze di trasparenza di cui all'articolo 12.⁵⁸

La comunicazione di una violazione dei dati deve soddisfare gli stessi requisiti, dettagliato sopra (in particolare per l'uso di un linguaggio chiaro e semplice), che si applicano a qualsiasi altra comunicazione con un soggetto di dati in relazione ai loro diritti o in connessione con la trasmissione di informazioni ai sensi degli articoli 13 e 14.

⁵⁶ Parere 03/2017 sul trattamento dei dati personali nel contesto di sistemi intelligenti di trasporto in cooperazione (C-ITS) - vedi paragrafo 4.2

⁵⁷ Orientamenti in materia di notifica delle violazioni dei dati personali ai sensi del regolamento 2016/679, WP 250

⁵⁸ Ciò è reso evidente dall'articolo 12.1, che si riferisce in particolare a "... qualsiasi comunicazione ai sensi degli articoli da 15 a 22 **e 34** relativa al trattamento alla persona ..." [enfasi aggiunta].

Annex

Information that must be provided to a data subject under Article 13 or Article 14

Required Information Type	Relevant article (if personal data collected directly from data subject)	Relevant article (if personal data not obtained from the data subject)	WP29 comments on information requirement
The identity and contact details of the controller and, where applicable, their representative ⁵⁹	Article 13.1(a)	Article 14.1(a)	This information should allow for easy identification of the controller and preferably allow for different forms of communications with the data controller (e.g. phone number, email, postal address, etc.)
Contact details for the data protection officer, where applicable	Article 13.1(b)	Article 14.1(b)	See WP29 Guidelines on Data Protection Officers ⁶⁰
The purposes and legal basis for the processing	Article 13.1(c)	Article 14.1(c)	In addition to setting out the purposes of the processing for which the personal data is intended, the relevant legal basis relied upon under Article 6 must be specified. In the case of special categories of personal data, the relevant provision of Article 9 (and where relevant, the applicable Union or Member State law under which the data is processed) should be specified. Where, pursuant to Article 10, personal data relating to criminal convictions and offences or related security

⁵⁹ As defined by Article 4.17 of the GDPR (and referenced in Recital 80), "representative" means a natural or legal person established in the EU who is designated by the controller or processor in writing under Article 27 and represents the controller or processor with regard to their respective obligations under the GDPR. This obligation applies where, in accordance with Article 3.2, the controller or processor is not established in the EU but processes the personal data of data subjects who are in the EU, and the processing relates to the offer of goods or services to, or monitoring of the behaviour of, data subjects in the EU.

⁶⁰ Guidelines on Data Protection Officers, WP243 rev.01, last revised and adopted on 5 April 2017

			misure basate sull'articolo 6.1 sono trattati, se del caso sotto il quale viene effettuata la lavorazione del pertinente diritto dell'Unione o degli Stati membri dovrebbe essere specificato.
Dove interessi legittimi (articolo 6.1 (f)) è la base giuridica per la trasformazione, il interessi legittimi perseguiti dal responsabile del trattamento o di un terzo	Articolo 13.1 (d)	Articolo 14.2 (b)	L'interesse specifico in questione deve essere identificato per il bene della persona. Come una questione di buone prassi, il controller può anche fornire il soggetto dei dati con le informazioni dal <i>test comparativo</i>, che deve essere effettuata per consentire richiamo all'art 6.1 (f) come base legale per l'elaborazione, in anticipo di qualsiasi raccolta degli interessati personale dati. Evitare informazioni dalla stanchezza, questo può essere incluso all'interno di un'istruzione più livelli di privacy / Avviso (vedere punto 35). In ogni caso, il WP29 posizione è quella informazioni alla persona interessata dovrebbe far capire che essi possono ottenere informazioni sul test comparativo su richiesta. Ciò è essenziale per un'effettiva trasparenza in cui dati soggetti hanno dubbi sul fatto che il test comparativo è stato eseguito abbastanza o che desiderano presentare un reclamo con un'autorità di vigilanza.
Categorie di dati personali in questione	Articolo non richiesto	14.1 (d)	Questa informazione è necessaria in uno scenario articolo 14 perché i dati personali non è stato ottenuto dalla persona interessata, che perciò manca un la consapevolezza di quali categorie di propri dati personali del titolare del trattamento ha ottenuto.

destinatari ⁶¹ (o categorie di destinatari) dei dati personali	Articolo 13.1 (e)	Articolo 14.1 (e)	Il termine “destinatario” è definita all'articolo 4.9 come <i>“Una persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo, a cui vengono comunicati i dati personali,</i> <i>se un terzo o no ” [enfasi aggiunta].</i> In quanto tale, un destinatario non deve essere una terza parte. Pertanto, altri controllori di dati, controller congiunte e trasformatori ai quali i dati sono trasmessi o divulgati sono coperti dal termine “destinatario” e informazioni su tali destinatari devono essere fornite in aggiunta alle informazioni sui destinatari di terze parti. L'attuale (nome) destinatari dei dati personali, o le categorie di destinatari, devono essere fornite. In conformità con il principio di equità, i controllori devono fornire informazioni sui destinatari quella è più significativo per gli interessati. In pratica, questo sarà generalmente i destinatari di nome, in modo che gli interessati sapere esattamente chi ha i propri dati personali. Se controllori scelgono di fornire le categorie di destinatari, le informazioni devono essere il più specifici possibile indicando il tipo di destinatario (ossia con riferimento alle attività che svolge), l'industria, settore e sottosettore e la posizione il destinatari.
Dettagli di trasferimenti a paesi terzi, il fatto della stessa ed i dettagli del relativo	Articolo 13.1 (f)	L'articolo 14.1 (f)	L'articolo in questione GDPR permettendo il trasferimento e il meccanismo corrispondente (ad esempio <u>decisione di adeguatezza ai sensi dell'articolo</u>

⁶¹ Ai sensi dell'articolo 4.9 del GDPR e si fa riferimento nel considerando 31

garanzie⁶² (includendo il esistenza o l'assenza di una Commissione adeguatezza decisione⁶³) ei mezzi per ottenere una copia di loro o quando sono stati resi disponibili			45 / norme vincolanti d'impresa ai sensi dell'articolo 47 clausole di protezione dei dati / standard di cui all'articolo 46.2 / deroghe e salvaguardie ai sensi dell'articolo 49, etc.) devono essere specificati. Le informazioni su dove e come il documento in questione può essere letta o ottenute dovrebbe essere fornita anche ad esempio fornendo un collegamento con il meccanismo utilizzato. In Secondo il principio di equità, il informazione disponibile su trasferimenti a paesi terzi dovrebbe essere come significativa possibile ai titolari dei dati; Questo in genere significa che i paesi terzi essere nominato.
Il periodo di conservazione (o se non è possibile, i criteri utilizzati per determinare tale periodo)	Articolo 13.2 (a)	Articolo 14.2 (a)	Questo è legato al requisito di minimizzazione dei dati in L'articolo 5.1 (c) e lo stoccaggio requisito di prescrizione di cui all'art 5.1 (e). Il periodo di conservazione (o criteri per determinare esso) può essere dettata da fattori ad esempio statuario requisiti o industria le linee guida, ma devono essere formulate in modo tale da consentire alla persona interessata di valutare, sulla base della propria situazione, ciò che il periodo di conservazione sarà per dati specifici / scopi. Non è sufficiente per il titolare genericamente stabiliscono che i dati personali saranno conservati per il tempo necessario ai fini legittimi del trattamento. Se del caso, i diversi periodi di conservazione dovrebbero essere stipulati per diverso

⁶² Come sancito dall'articolo 46.2 e 46.3

⁶³ Ai sensi dell'articolo 45

			categorie di dati personali e / o diverse finalità, anche quando <u>appropriati, periodi archiviazione.</u>
I diritti della persona interessata a: • accesso; • rettifica; • la cancellazione; • restrizione trasformazione; • opposizione al trattamento e • portabilità.	Articolo 13.2 (b)	Articolo 14.2 (c)	Questo informazioni dovrebbero essere specifico allo scenario di trasformazione e comprendono una sintesi di ciò che il diritto comporta e come la persona interessata può adottare misure per esercitarlo e le eventuali limitazioni a destra (vedi punto 68). In particolare, il diritto di opporsi al trattamento deve essere esplicitamente portato all'attenzione della persona interessata, al più tardi al momento della prima comunicazione con la persona interessata e deve essere presentato in modo chiaro e separato da qualsiasi altra informazione. ⁶⁴ In relazione al diritto alla portabilità, vedere Linee guida WP29 sul diritto alla portabilità dei dati. ⁶⁵
Se la trasformazione è basata sul consenso (o il consenso esplicito), il diritto di ritirare il consenso in qualsiasi momento	Articolo 13.2 (c)	Articolo 14.2 (d)	Queste informazioni dovrebbero comprendere come il consenso può essere ritirato, tenendo conto che dovrebbe essere facile per un soggetto di dati di ritirare il consenso da dare. ⁶⁶
Il diritto di presentare una denuncia presso l'autorità di vigilanza	Articolo 13.2 (d)	Articolo 14.2 (e)	Queste informazioni dovrebbero spiegare che, a norma dell'articolo 77, l'interessato ha il diritto di presentare un reclamo con una vigilanza autorità, in particolare nello Stato membro della sua residenza abituale, luogo di lavoro o di una presunta violazione del GDPR.
Se c'è una legge o di contratto obbligo di fornire le informazioni o <u>se è necessario</u>	Articolo 13.2 (e)	Non necessario,	ad esempio in un impiego contesto, può essere un requisito contrattuale a fornire determinati

⁶⁴ Articolo 21.4 e il considerando 70 (che si applica nel caso di direct marketing)

⁶⁵ Orientamenti in materia di diritto alla portabilità dei dati, WP 242 rev.01, lo scorso rivisti e adottate il 5 Aprile 2017

⁶⁶ Articolo 7.3

accedere in un contratto o se vi sia l'obbligo di fornire le informazioni e le possibili conseguenze del fallimento.			informazioni a un datore di lavoro attuale o prospettico. Moduli online dovrebbero identificare chiaramente che i campi siamo “Necessaria”, che non sono, e quali saranno le conseguenze di <u>non compilando i campi richiesti.</u>
La fonte da cui i dati personali hanno origine, e se del caso, sia che proveniva da una fonte accessibile al pubblico	Articolo non richiesto	14.2 (f)	La fonte specifica dei dati dovrebbe essere fornita a meno che non sia possibile farlo - vedi ulteriori indicazioni al paragrafo 60. Se la fonte specifica non è nominato poi informazione a condizione dovrebbe includere: la natura delle fonti (vale a dire pubblicamente / fonti a capitale privato) e il tipo di organizzazione / industria / settore.
L'esistenza del processo decisionale automatizzato Compreso profilatura e, conseguenze se del caso, informazioni significative sulla logica utilizzata e il significato e la prevista di come <u>elaborazione per la persona</u>	Articolo 13.2 (f)	Articolo 14.2 (g)	Vedere Linee guida WP29 sul processo decisionale individuale automatizzata e Profiling.⁶⁷

⁶⁷ Orientamenti in materia di Automated individuale decisionali e Profiling ai fini del regolamento 2016/679, WP 251