G – EUROPRIVACY GDPR CORE CRITERIA

Org. di Cert.:
Richiedente:
Target of Evaluation:
Nome dell'Esperto:
Data:

I "Mezzi di Verifica Suggeriti", compresi i documenti di riferimento, devono essere valutati in base ai criteri fino a quando non vengono raccolte prove sufficienti per determinare se i criteri sono soddisfatti.

Come promemoria generale, ogni criterio applicabile deve essere valutato singolarmente e deve essere soddisfatto. Qualsiasi criterio non soddisfatto determina una non conformità formale, anche se gli altri criteri sono soddisfatti.

La valutazione dei criteri deve essere effettuata in conformità con la Specifica Generale e i Requisiti dello Schema di Certificazione Europrivacy (in particolare la sezione 12) e con le Linee Guida Europrivacy sull'Uso di Criteri, Verifiche e Controlli, entrambi documenti disponibili su Europrivacy community website.

"Autorità di Controllo" si riferisce all'autorità nazionale per la protezione dei dati.

Ref ID	Richiedente	Specifico/Generico	Livello	TITOLO	CRITERI applicabili al Target of Evaluation (clausole prescrittive)	GUIDA ALL'ATTUAZIONE (clausole informative)	Mezzi di verifica suggeriti (per l'Auditor)	GDPR Art.
G.1				**Liceità del trattamento dei dati** Obiettivo: Garantire che il trattamento dei dati nell'ambito del Target of Evaluation sia legittimo e proporzionato. Condizione: SE il Richiedente è il Titolare del trattamento dei dati personali trattati nel Target of Evaluation ALLORA:				
G.1.1				**Liceità del trattamento**				
G.1.1.1	C	S	A	Valutazione della liceità del trattamento	A) Deve esistere una relazione o un documento scritto che dimostri che il trattamento dei dati nel Target of Evaluation è stato giudicato legittimo dal DPO del Richiedente o da un esperto legale con competenze adeguate. E B) Se la legittimità è subordinata ad azioni correttive, il Richiedente dovrà implementarle. E C) Il report di valutazione (o rivalutazione) della legittimità deve: c.1) coprire tutti i trattamenti di dati personali specificati nel Target of Evaluation; c.2) (E) indicare la base giuridica del trattamento dei dati; c.3) (E) se applicabile, includere i documenti giustificativi o i riferimenti; c.4) (E) sono stati eseguiti negli ultimi 12 mesi prima della valutazione iniziale.	Il Richiedente può stabilire regole o una procedura formale per valutare la liceità del trattamento dei dati prima di effettuarlo. Il DPO del Richiedente è tenuto a valutare la liceità del trattamento dei dati. Nel valutare la liceità, si deve tenere conto del principio di proporzionalità per garantire che il trattamento dei dati non vada oltre la sua finalità legittima. Il consenso deve essere esplicito e richiede un'azione inequivocabile da parte dell'interessato per esprimere il proprio consenso. Non sono accettabili, ad esempio, caselle di controllo preselezionate. In caso di dubbi sulla qualifica dell'esperto o sulla conclusione della valutazione, l'Auditor deve contestare la relazione e richiedere una valutazione complementare.	Registrazione e documentazione della valutazione di legittimità e della convalida. Intervista del DPO. Dichiarazione scritta del DPO o dello studio legale.	6.1

G.1.1.2	C	S	A	Giustificazione della legittimità	Il trattamento dei dati deve essere conforme ad almeno una delle seguenti motivazioni:	Il Richiedente deve documentare e dimostrare la liceità del trattamento dei dati personali in quanto conforme a una delle seguenti basi giuridiche di liceità. Si raccomanda di stabilire regole, policy, processi o meccanismi per garantire e dimostrare che ogni attività di trattamento dei dati personali risponda ad almeno una delle seguenti basi giuridiche prima di effettuare le attività di trattamento.		6.1
				Consenso	A) Il trattamento dei dati si basa sul consenso informato degli interessati. che: a.1) deve essere raccolto prima di trattare i loro dati personali; a.2) (E) deve essere conferito dall'interessato in modo chiaro ed esplicito (con una chiara azione affermativa).	Questo criterio deve essere valutato in base al criterio dettagliato G.1.2.1. Affinché il consenso sia valido, gli interessati devono acconsentire al trattamento dei loro dati personali per una o più finalità specifiche. Il Richiedente può definire e implementare policy, procedure e/o meccanismi interni per inquadrare il meccanismo di raccolta del consenso e garantire che il consenso sia: - liberamente dato; - per scopi specifici; - informato; - inequivocabile; - basato su una dichiarazione o su una chiara azione affermativa; - richiesto prima del trattamento dei dati. Ove applicabile, il Richiedente deve istituire un registro elettronico dei consensi raccolti, che includa la data e l'ora del consenso dato. Se il consenso è la base per il trattamento dei dati, devono essere implementate regole, procedure o meccanismi appropriati per impedire il trattamento dei dati personali quando il consenso non è stato ottenuto o è stato ritirato.	Registrazione del consenso dell'interessato. Interfaccia utente. Accordo/clausole contrattuali.	6.1.a
				Necessità contrattuale	O B) Il trattamento dei dati è necessario per l'esecuzione dei servizi specificati nel contratto.	Il Richiedente deve documentare ed essere in grado di dimostrare che il trattamento dei dati è proporzionato e necessario per eseguire il contratto o la richiesta. Il Richiedente deve stabilire regole, policy, processi o meccanismi per dimostrare e documentare la necessità contrattuale che fonda l'utilizzo di questa base giuridica. Si raccomanda il coinvolgimento del DPO (valutazione e convalida) in questo processo.	Base contrattuale. Valutazione della necessità contrattuale da parte del DPO o di uno studio legale. Intervista del DPO.	6.1.b
				Obbligo legale	O C) Il Richiedente deve dimostrare l'esistenza di un obbligo legale che prevede il trattamento di dati.	Il Richiedente deve essere in grado di dimostrare che: - il trattamento è necessario per l'adempimento dell'obbligo legale (non sono disponibili metodi meno invasivi); - il trattamento è proporzionato all'obbligo legale (vengono raccolti e trattati solo i dati personali adeguati e pertinenti alle finalità del trattamento).	Base giuridica. Registro o documentazione della valutazione di legittimità. Intervista del DPO.	6.1. c
				Interessi vitali	O D) Il trattamento dei dati deve essere necessario per tutelare interessi vitali degli interessati (ad es. vita, salute);	Il Richiedente deve essere in grado di dimostrare che il trattamento dei dati: - è necessario e proporzionato per proteggere gli interessi vitali rivendicati (non era disponibile un metodo meno intrusivo per ottenere lo stesso risultato); - è proporzionato alla tutela degli interessi vitali rivendicati (vengono raccolti e trattati solo i dati personali adeguati e pertinenti alle finalità del trattamento).	Registro o documentazione della valutazione di legittimità. Intervista del DPO.	6.1.d
				Interesse pubblico o pubblici poteri	O E) Il Richiedente deve dimostrare che il trattamento dei dati: e.1) si basa sull'interesse pubblico o sui pubblici poteri; e.2) (E) con la documentazione relativa alla base giuridica per tale interesse pubblico o autorità ufficiale.	Il Richiedente deve conservare i registri che dimostrano che il compito o la funzione: - fornisce un chiaro mandato per eseguire il relativo trattamento dei dati; - (E) il trattamento è necessario e proporzionato per l'esecuzione del compito (nessun metodo meno invasivo potrebbe portare allo stesso risultato).	Base giuridica o decisione amministrativa. Registro o documentazione della valutazione di legittimità. Intervista del DPO.	6.1.e. 6.3

			Interessi legittimi	O F) Il trattamento dei dati si basa su interessi legittimi per i quali il Richiedente deve dimostrare: f.1) la descrizione scritta dell'interesse legittimo rivendicato; f.2) (E) il DPO o un esperto legale con competenze adeguate ha valutato per iscritto l'impatto del trattamento dei dati sui diritti e le libertà degli interessati; f.3) (E) il DPO o un esperto legale con competenze adeguate ha concluso per iscritto che l'interesse legittimo non veda prevalere i diritti e le libertà degli interessati.	Il Richiedente deve disporre di processi per: - valutare e documentare gli interessi degli interessati; - identificare e documentare il trattamento dei dati personali dei minori di età. I registri devono documentare: - l'interesse specifico e legittimo perseguito dal trattamento dei dati; - la valutazione dell'applicabilità dell'interesse legittimo rivendicato per svolgere le attività di trattamento; - la valutazione degli interessi e delle libertà dell'interessato; - la valutazione delle ragionevoli aspettative dell'interessato in merito all'ulteriore trattamento dei dati personali; - la convalida da parte del DPO del legittimo interesse; - il trattamento è necessario e proporzionato alle finalità coinvolte negli interessi legittimi rivendicati (non era disponibile un metodo meno intrusivo per raggiungere lo stesso risultato). La Corte di giustizia dell'Unione europea ha confermato l'approccio tripartito (finalità, necessità, bilanciamento) per il test degli interessi legittimi con il caso Rigas (C-13/16, 4 maggio 2017) nel contesto della protezione dei dati personali. Direttiva 95/46/CE.	Documentazione relativa al legittimo interesse. Registro o documentazione della valutazione di legittimità. Intervista del DPO.	6.1.f

G.1.1.3	C	S	A	Conformità alle normative nazionali	A) Un esperto legale deve aver valutato la conformità del trattamento dei dati con gli obblighi nazionali complementari in materia di protezione dei dati personali applicabili al Richiedente e ha fornito la sua valutazione nel National Obligations Compliance Assessment Report (NOCAR). E B) Il NOCAR deve contenere: b.1) una chiara identificazione del Target of Evaluation che è stato valutato; b.2) (E) la descrizione della qualifica dell'esperto legale; b.3) (E) l'elenco degli obblighi nazionali complementari di protezione dei dati identificati che sono applicabili al Target of Evaluation; b.4) (E) la valutazione della conformità del Target of Evaluation con gli obblighi nazionali complementari identificati; b.5) (E) nel caso in cui i dati siano trattati a fini di archiviazione, ricerca o statistica, la misure tecniche e organizzative implementate per il rispetto dei diritti fondamentali e degli interessi degli interessati, in particolare le misure di minimizzazione dei dati; b.6) (E) se la valutazione conclude che sono necessarie azioni per conformarsi a gli obblighi nazionali, tali azioni devono essere documentate. E C) L'esperto legale deve: c.1) avere preso in considerazione almeno di tutti gli obblighi nazionali complementari applicabili elencati negli Obblighi Nazionali di Protezione dei Dati resi disponibili dall'ECCP; c.2) (E) avere verificato se altre leggi e regolamenti nazionali specifici del dominio sono applicabili; c.3) (E) avere verificato se il trattamento dei dati richiede un'autorizzazione nazionale, e in tal caso avere verificato la validità dell'autorizzazione richiesta. E D) Il NOCAR deve: d.1) essere completo e coerente; d.2) (E) concludere che il Target of Evaluation è conforme agli obblighi nazionali. E E) Il Richiedente deve: a.1) essersi impegnato ad applicare nel tempo le misure documentate nel report NOCAR; a.2) (E) se applicabile, avere stabilito un piano d'azione dettagliato per conformarsi alle misure raccomandate dal NOCAR; a.3) (E) laddove applicabile, avere applicato e documentato le azioni contenute nel piano d'azione necessario per ottemperare agli obblighi nazionali.	Le normative nazionali comportano obblighi complementari di protezione dei dati da rispettare. Un esperto legale con competenze adeguate nella normativa nazionale applicabile deve valutare se le attività di trattamento dei dati da certificare sono conformi alle legislazioni e alle normative nazionali complementari applicabili, comprese quelle specifiche del dominio. Questa valutazione può essere effettuata da un esperto interno o esterno, compreso il DPO del Richiedente, se ha le competenze legali richieste nella normativa nazionale applicabile e non è in conflitto con i suoi requisiti di indipendenza. L'ECCP fornisce le "Linee Guida Europrivacy sul National Obligations Compliance Assessment Report" (NOCAR), che illustrano in dettaglio il contenuto e la struttura del report da redigere. Gli Auditor devono esaminare il NOCAR e stabilire, in base al suo contenuto, se è completo, soddisfacente e coerente, e rifiutarlo se ritengono, sulla base dei fatti, che il report e le sue conclusioni non siano affidabili. L'ECCP fornisce anche elenchi di requisiti nazionali complementari identificati (National Data Protection Obligations profiles), messi a disposizione di tutti i richiedenti e gli auditor di Europrivacy, al fine di garantire che gli obblighi nazionali fondamentali non vengano dimenticati durante la valutazione e la revisione del NOCAR. La valutazione deve considerare se il trattamento dei dati è soggetto ad autorizzazione da parte delle autorità nazionali e convalidare che tale autorizzazione sia stata concessa. I trattamenti di dati che coinvolgono categorie particolari di dati, la videosorveglianza, le installazioni di Internet of Things negli spazi pubblici o i cookie dei siti web sono probabilmente soggetti a obblighi nazionali specifici e a potenziali autorizzazioni che devono essere verificate. Gli obblighi nazionali possono anche avere un impatto su diversi criteri, come i requisiti di sicurezza, la valutazione dell'impatto sulla protezione dei dati, la data protection by design e by default, etc. Nel caso in cui il report NOCAR specifichi le misure correttive che il Richiedente deve adottare, quest'ultimo dovrà produrre un piano d'azione correttivo dettagliato. L'organismo di certificazione non limiterà la sua valutazione all'attuazione delle misure raccomandate definite dall'esperto legale. L'organismo di certificazione ha il compito di verificare che il richiedente abbia attuato le misure documentate nel NOCAR (indipendentemente dal fatto che siano state attuate o meno prima che l'esperto legale effettuasse la propria valutazione). Quando i dati sono trattati a fini di archiviazione nel pubblico interesse, a fini di ricerca scientifica o storica o a fini statistici, vi è l'obbligo di adottare misure specifiche per la minimizzazione dei dati, come la pseudonimizzazione o l'anonimizzazione al fine di rispettare i diritti e gli interessi fondamentali degli interessati (come richiesto dall'articolo 89 del GDPR). L'effettiva implementazione di questi requisiti sarà verificata dal Criterio G.6.1.1. L'adeguatezza delle misure richieste in b5) è verificata attraverso il criterio G.6.1.1 "Data protection by design and by default". Inoltre, la NOCAR deve affrontare gli obblighi nazionali complementari applicabili al trattamento dei dati a fini di archiviazione, ricerca o statistica.	Revisione del National Obligation Compliance Assessment Report (NOCAR).	6.2, 6.3, 89
G.1.1.4	C	S	A	Adeguata qualificazione dell'esperto	A) L'esperto legale che ha preparato il National Obligation Compliance Assessment Report (NOCAR) deve avere: a.1) un Master of Laws (LL.M.) o una qualifica di livello equivalente, o una significativa esperienza professionale nella protezione dei dati; a.2) (E) competenza o esperienza pratica documentata di diritto nazionale di cui si occupa il NOCAR; a.3) (E) conoscenza della legge sulla protezione dei dati.	L'esperto legale deve possedere un'adeguata competenza in materia di leggi e regolamenti nazionali da valutare all'interno del National Obligations Compliance Assessment Report. È essenziale che tali esperti legali dimostrino il loro livello di competenza nelle normative nazionali applicabili. Il livello di competenza previsto dovrebbe essere almeno equivalente alla qualifica richiesta per gli esperti legali che partecipano alle attività di audit e certificazione ai sensi degli artt. 42 e 43 del GDPR secondo le linee guida dell'EDPB o secondo la normativa nazionale applicabile.	Esame della documentazione del NOCAR e delle qualifiche dell'esperto.	6.2, 6.3

G.1.2				**Requisiti complementari per la validità del consenso (se applicabile)**				**7**
				Condizione:	SE la liceità del trattamento dei dati si basa sul consenso ALLORA:			
G.1.2.1	C	S	A	Requisiti formali per il consenso	A) Il consenso degli interessati deve essere preventivo e informato, garantendo che: a.1) le informazioni sulle finalità del trattamento dei dati e sull'identità del Titolare del trattamento devono essere comunicate agli interessati prima o al momento del rilascio del consenso; a.2) (E) il consenso deve essere richiesto per una finalità specifica; a.3) (E) la richiesta di consenso deve essere formulata in modo facilmente comprensibile; a.4) (E) se formulata in forma scritta, la richiesta di consenso deve essere presentata sotto forma di paragrafo separato e distinguibile da altre questioni; a.5) (E) il consenso deve essere raccolto prima che il Richiedente tratti i dati personali; a.6) (E) il consenso deve essere dato dagli interessati in modo chiaro ed esplicito (con una chiara azione affermativa). E B) Il consenso degli interessati deve essere dato liberamente, anche garantendo che: b.1) gli interessati possono limitare o rinunciare a prestare il proprio consenso senza che ciò comporti effetti negativi su di loro; b.2) (E) se il Target of Evaluation comprende diverse finalità per i trattamenti di dati il Richiedente dovrà fornire un meccanismo di raccolta del consenso granulare che consenta all'interessato di scegliere liberamente a quale finalità acconsentire; b.3) (E) se il Richiedente è un'autorità pubblica o un datore di lavoro dell'interessato, il consenso non deve essere soggetto a uno squilibrio di potere.	Il Richiedente deve tenere presente che le caselle pre-selezionate non sono riconosciute come un consenso valido alla luce del GDPR (art. 5-6 GDPR). Il consenso richiede una "indicazione" inequivocabile della volontà dell'interessato di acconsentire al trattamento dei dati. Solo un comportamento attivo da parte dell'interessato al fine di dare il proprio consenso può soddisfare tale requisito. Il GDPR esclude che "il silenzio, le caselle pre-selezionate o l'inattività" possano costituire consenso. Quando si utilizzano plugin e microservizi per servizi, applicazioni o interfacce utente online, il Richiedente deve assicurarsi che tali plugin e microservizi siano conformi al GDPR e siano chiaramente comunicati agli interessati. Qualsiasi parte di tale dichiarazione che costituisca una violazione del presente regolamento non dovrebbe essere vincolante. Si raccomanda di rendere disponibile la procedura di consenso nelle varie lingue nazionali dei territori in cui il Titolare del trattamento intende raccogliere attivamente i consensi.	Procedura, interfaccia utente o meccanismo utilizzato per raccogliere il consenso. Dimostrazione da parte del DPO. Test della procedura.	7.2
G.1.2.2	C	S	A	Assenza di vincoli inutili per il consenso	A) Se il Target of Evaluation comprende diverse finalità distinte del trattamento dei dati, ALLORA il Richiedente deve fornire un meccanismo di raccolta del consenso granulare che consenta all'interessato di di scegliere liberamente a quale finalità acconsentire.	Il meccanismo di raccolta del consenso deve evitare qualsiasi vincolo. Come principio generale, il consenso richiesto deve rimanere proporzionato alla finalità del trattamento dei dati.	Procedura, interfaccia utente o meccanismo utilizzato per raccogliere il consenso. Dimostrazione da parte del DPO.	7.4
G.1.2.3	C	S	A	Diritto di revoca del consenso	A) Il Richiedente dovrà dimostrare che la procedura o il meccanismo in atto per conformarsi con il diritto dell'interessato di revocare il consenso permetta di attuare efficacemente tale richiesta. E B) La procedura per la revoca del consenso dovrebbe essere: b.1) semplice come quella utilizzata per la raccolta del consenso; b.2) (E) accessibile attraverso le interfacce utente utilizzate per raccogliere il consenso.	Il Richiedente deve chiedere al proprio DPO di esaminare e convalidare le policy, le procedure, le linee guida e i meccanismi interni di gestione della revoca del consenso. Da notare che la revoca del consenso non pregiudica la liceità del trattamento basato sul consenso prima della sua revoca. Prima di dare il consenso, l'interessato deve essere informato.	Procedura, interfaccia utente o meccanismo utilizzato per revocare il consenso. Dimostrazione da parte del DPO.	7.3
G1.3				**Condizioni applicabili al consenso di un minore in relazione ai servizi della società dell'informazione (se applicabile)**				**8**
				Condizione:	SE l'obiettivo della valutazione comprende servizi della società dell'informazione offerti direttamente a bambini di età inferiore ai 16 anni, ALLORA:			
G.1.3.1	C	S	A	Liceità del trattamento dei dati dei minori di età e Verifica del consenso dei genitori	A) I limiti di età applicabili per il consenso devono essere chiaramente comunicati ai potenziali nuovi interessati coinvolti nel trattamento dei dati. E B) Esiste una procedura e/o un meccanismo: b.1) per richiedere l'età degli interessati minorenni; b.2) (E) per bloccare la raccolta di dati personali di minori di età inferiore a quella di consenso OPPURE per richiedere il consenso del titolare della responsabilità genitoriale per il minore al di sotto dell'età del consenso.	Quando offre servizi a minori di età, il Richiedente è incoraggiato a creare un registro elettronico dei consensi raccolti, che includa la data e l'ora dei consensi rilasciati. Il consenso deve essere esplicito e richiede una conferma inequivocabile dal titolare della potestà genitoriale. Per la procedura di registrazione online, il Richiedente può richiedere un'e-mail di conferma al titolare della potestà genitoriale. Il Richiedente deve tenere conto delle normative nazionali applicabili che possono stabilire un limite di età diverso. Gli Stati membri possono prevedere per legge un'età inferiore per questi scopi, a condizione che tale età inferiore non sia inferiore a 13 anni.	Procedura, interfaccia utente o meccanismo utilizzato per raccogliere il consenso. Dimostrazione da parte del DPO.	8.1, 8.2

G.2				**Trattamento di dati particolari** Obiettivo: Garantire che le categorie particolari di dati che verrebbero trattate nell'ambito del Target of Evaluation siano conformi ai requisiti normativi.				
G.2.1				**Adeguatezza del trattamento di categorie particolari di dati** Condizione: SE il Target of Evaluation tratta categorie particolari di dati personali, ALLORA:				**9**
G.2.1.1	C	S	A	Categorie particolari di dati - Convalida del DPO	A) Il DPO o un esperto con competenze adeguate: a.1) ha valutato i rischi e l'impatto del trattamento delle categorie particolari di dati sui diritti, le libertà e gli interessi legittimi degli interessati; a.2) (E) ha confermato la liceità del trattamento delle categorie particolari di dati, anche rispetto agli obblighi nazionali applicabili.	Il Richiedente deve fare un registro sistematico delle categorie di dati trattati nel Target of Evaluation. Il trattamento di categorie particolari di dati deve essere attentamente analizzato dal DPO. Particolare attenzione deve essere prestata all'analisi dei rischi per i diritti e la libertà degli interessati.	Valutazione del rischio e relazione di valutazione della legittimità da parte del DPO. Report NOCAR.	9
G.2.1.2	C	S	A	Base giuridica per il trattamento di categorie particolari di dati	Il Richiedente deve dimostrare che il trattamento di Categorie Particolari di Dati Personali nel Target of Evaluation sono leciti in base ad almeno una delle seguenti giustificazioni:	Il Richiedente deve richiedere al proprio DPO di verificare e convalidare specificamente che il trattamento di qualsiasi categoria speciale di dati: - è conforme ai requisiti del GDPR e alle normative nazionali applicabili; - e, ove richiesto, è stato autorizzato.	Relazione di valutazione della legittimità. Report NOCAR. Intervista al DPO.	9
				Consenso esplicito	A) Il Richiedente deve dimostrare che il trattamento delle categorie particolari di dati si basa sul consenso esplicito degli interessati.	Il Richiedente può richiedere al proprio DPO di esaminare e convalidare le policy, le procedure, le linee guida e i meccanismi interni di gestione del consenso. Il DPO deve verificare e garantire che il trattamento sia conforme agli obblighi nazionali applicabili.	Procedura, interfaccia utente o meccanismo utilizzato per raccogliere il consenso.	9.2.a
				Occupazione, previdenza sociale e protezione	O B) Il Richiedente deve dimostrare che il trattamento di categorie particolari di dati è basato su esigenze lavorative e sociali.	Il Richiedente deve conservare i registri per dimostrare che il trattamento dei dati: - riguarda il settore dell'impiego o quello del diritto della previdenza o della protezione sociale; - è finalizzato all'adempimento di obblighi o all'esercizio di specifici diritti del Titolare o dell'interessato; - è necessario e proporzionato per lo svolgimento del compito (nessun metodo meno invasivo potrebbe portare allo stesso risultato); - fornisce adeguate garanzie per i diritti fondamentali e gli interessi delle persone interessate.	Documentazione legale o amministrativa.	9.2.b
				Interesse vitale	O C) Il Richiedente deve dimostrare che il trattamento di categorie particolari di dati è basato su interessi vitali quando: c.1) gli interessi vitali degli interessati erano a rischio (vita, salute); c.2) (E) i relativi interessati o le persone fisiche protette sono stati fisicamente o legalmente incapaci di fornire il proprio consenso.	Il Richiedente deve tenere una documentazione che dimostri che: - gli interessi vitali delle persone interessate erano a rischio (vita, salute); - il trattamento è necessario e proporzionato per lo svolgimento dell'incarico (nessun metodo meno invasivo potrebbe portare allo stesso risultato); - l'interessato o la persona fisica protetta è fisicamente o legalmente incapace di fornire il proprio consenso; - il DPO ha convalidato la procedura per tale trattamento basato sull'interesse vitale.	Registrazione e documentazione della valutazione degli interessi vitali e del processo decisionale. Intervista del DPO.	9.2.c
				Ente non profit con scopo legittimo	O D) Il Richiedente deve dimostrare che il trattamento di categorie particolari di dati è basati su attività senza scopo di lucro in cui: d.1) il Richiedente è un'entità senza scopo di lucro; d.2) (E) i dati trattati riguardano esclusivamente i soci e gli ex soci del Richiedente e/o le persone che hanno contatti regolari con il Richiedente in relazione alle finalità da questo perseguite; d.3) (E) devono essere in vigore norme e/o procedure interne per evitare che i dati personali vengono divulgati a terzi senza il consenso dell'interessato.	Il Richiedente deve garantire che il trattamento dei dati rimanga proporzionato alle finalità che gli interessati possono aspettarsi dal Richiedente.	Statuto dell'organizzazione. Registro delle attività di trattamento. Intervista dei dipendenti e del DPO. Regole e linee guida interne.	9.2.d

				Dati pubblici	O E) Il Richiedente deve dimostrare che il trattamento di categorie particolari di dati si basa su dati palesemente resi pubblici dagli interessati.	Il Richiedente deve essere in grado di dimostrare che i dati sono palesemente resi pubblici dagli interessati.	Documentazione sulla raccolta dei dati. Registro delle attività di trattamento. Analisi del campione di dati. Intervista dei dipendenti e del DPO.	9.2.e
				Azioni legali	O F) Il Richiedente deve dimostrare che il trattamento di categorie particolari di dati è necessario per l'instaurazione, l'esercizio o la difesa di pretese legali, o per agire di fronte a un tribunale nella propria capacità di agire.	Il Richiedente deve avere prove documentate di azioni legali imminenti o in corso.	Documentazione relativa a pretese legali e azioni giudiziarie. Intervista dei dipendenti e del DPO.	9.2.f
				Interesse pubblico	O G) Il Richiedente deve dimostrare che il trattamento di categorie particolari di dati è necessario per motivi di interesse pubblico, laddove: g.1) l'interesse pubblico si basa sul diritto dell'Unione o degli Stati membri; g.2) (E) devono essere state adottate misure specifiche per la tutela dei diritti fondamentali e gli interessi degli interessati.	Il Richiedente deve conservare i registri o le prove per dimostrare che: - il DPO o il top management hanno contribuito alla valutazione del rischio per i diritti, le libertà e gli interessi legittimi dell'interessato; - il trattamento dei dati è necessario e proporzionato per l'esecuzione del compito.	Documentazione sull'interesse pubblico, compresa la base giuridica/amministrativa. Intervista del DPO. Documentazione della valutazione di legittimità da parte del DPO.	9.2.g
				Salute e capacità lavorativa	O H) Il Richiedente deve dimostrare che il trattamento di categorie particolari di dati è necessari per scopi di assistenza medica o sociale, laddove h.1) il trattamento deve riguardare una delle seguenti attività: medicina preventiva o del lavoro; valutazione della capacità lavorativa del dipendente; diagnosi; fornitura di assistenza o trattamento sanitario o sociale; gestione dei sistemi e servizi di assistenza sanitaria o sociale; h.2) (E) i dati devono essere trattati da o sotto la responsabilità di un professionista soggetto all'obbligo del segreto professionale.	Il Richiedente deve tenere registri o prove per dimostrare che: - il trattamento si basa su una base giuridica o su un contratto con un professionista sanitario; - il trattamento è necessario e proporzionato per lo svolgimento del compito (nessun metodo meno invasivo potrebbe portare allo stesso risultato); - i professionisti sono soggetti all'obbligo di segretezza del Responsabile del trattamento.	Registrazione e documentazione della valutazione di legittimità. Intervista del DPO. Clausole contrattuali dei dipendenti. Regole interne.	9.2.h
				Salute pubblica	O I) Il Richiedente deve dimostrare che il trattamento di categorie particolari di dati è necessario per motivi di interesse pubblico nell'ambito della salute pubblica, laddove: i.1) l'interesse pubblico nel settore della salute pubblica si basa su una base giuridica; i.2) (E) i dati sono trattati da o sotto la responsabilità di un professionista soggetto all'obbligo del segreto professionale.	Le misure di protezione dei diritti e degli interessi dell'interessato possono includere policy, processi o meccanismi per garantire che: - il Richiedente ha valutato i rischi e bilanciato la decisione di trattare le categorie particolari di dati con i diritti, le libertà e gli interessi legittimi degli interessati; - il personale del Richiedente che ha accesso alle categorie particolari di dati è tenuto al segreto professionale.	Documentazione sull'interesse pubblico. Intervista del DPO. Base giuridica o amministrativa. Registrazione e documentazione della valutazione di legittimità.	9.2.i
				Finalità di archiviazione, ricerca e statistica	O J) Il Richiedente deve dimostrare che il trattamento di categorie particolari di dati è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica, o a fini statistici, laddove: j.1) il DPO deve aver valutato e confermato che i dati trattati sono utili e proporzionati alla finalità dichiarata; j.2) (E) devono essere fornite informazioni pubbliche sulle finalità delle attività di trattamento dei dati con un canale di contatto per gli interessati; j.3) (E) devono essere state adottate misure specifiche per proteggere i diritti e gli interessi degli interessati, come le tecniche di pseudonimizzazione e anonimizzazione.	Le misure di protezione dei diritti e degli interessi dell'interessato possono includere policy, processi o meccanismi per garantire che: - il DPO e/o il top management hanno valutato i rischi per i diritti, le libertà e gli interessi legittimi degli interessati; - se compatibile con i requisiti associati alle finalità del trattamento, le categorie particolari di dati sono state pseudonimizzate o rese anonime; - le misure di sicurezza implementate sono state convalidate dal DPO.	Documentazione del progetto, comprese le informazioni online. Documentazione della valutazione di legittimità da parte del DPO.	9.2.j

G.2.2				**Trattamento dei dati relativi a condanne penali e reati (se applicabile)**				**10**
				Condizione:	SE il Target of Evaluation mira a trattare dati relativi a condanne penali e/o reati, ALLORA:			
G.2.2.1	C	S	A	Dati relativi a condanne penali e reati	A) Il Richiedente dovrà dimostrare che il trattamento dei dati personali relativi a condanne penali e reati: a.1) deve essere effettuato sotto il controllo dei pubblici poteri, o deve essere specificamente autorizzato da una legge dell'Unione o degli Stati membri che è chiaramente identificata, o dovrà essere strettamente limitato e basato su un interesse legittimo (come i processi di assunzione); a.2) (E) non deve costituisce un registro completo delle condanne penali, salvo se tenuto sotto il controllo dei pubblici poteri. E B) Il trattamento dei dati relativi a condanne penali e/o reati deve essere stato: b.1) valutato da un esperto legale qualificato come conforme agli obblighi previsti dalla normativa nazionale applicabile; b.2) (E) controllato e valutato conforme dal DPO; b.3) (E) approvato dalla direzione del Richiedente.	Il Richiedente deve documentare la base giuridica che autorizza il trattamento dei dati relativi a condanne penali e reati. La documentazione deve identificare chiaramente la normativa nazionale applicabile. Il trattamento dei dati relativi a condanne penali e reati deve basarsi su una chiara base giuridica o su un'autorizzazione formale da parte di un'autorità nazionale o europea competente. In caso contrario, il trattamento dei dati non deve essere certificato. La valutazione deve far parte del National Obligation Compliance Assessment Report (NOCAR) preparato per valutare la conformità al criterio G.1.1.3 sugli obblighi nazionali.	Documentazione della valutazione di legittimità da parte del DPO o di un esperto legale qualificato (National Obligation Compliance Assessment Report). Intervista dei dipendenti e del DPO.	10
G.3				**Diritti degli interessati**				
				Obiettivo:	Garantire che il trattamento dei dati nell'ambito del Target of Evaluation rispetti e consenta l'effettivo esercizio dei diritti degli interessati.			
G.3.1				**Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti degli interessati**				**12**
G.3.1.1	C	S	A	Obbligo di informare con un linguaggio chiaro	A) Le informazioni sul trattamento dei dati fornite dal Richiedente agli interessati e alle parti interessate sono: a.1) comprensibili in un linguaggio chiaro e semplice; a.2) (E) disponibili nella lingua nazionale ufficiale del Richiedente; a.3) (E) disponibili nella lingua degli interessati. E B) SE il Target of Evaluation è destinato al trattamento di dati personali di minori di età, ALLORA il DPO deve aver valutato e convalidato l'adeguatezza della formulazione delle informazioni rispetto alla capacità di comprensione dei minori di età.	Il Richiedente deve fornire le informazioni in modo conciso, trasparente, comprensibile e facilmente accessibile, in un linguaggio chiaro e semplice e in forma scritta (vedi: Linee guida WP29 WP260 Rev. 01): - concise e trasparenti: le informazioni devono essere efficienti e sintetiche per evitare l'affaticamento informativo; - intelligibili: le informazioni devono essere comprese da un membro medio del pubblico a cui sono destinate; - facilmente accessibili: l'interessato non deve cercare le informazioni, ma deve trovarle immediatamente; - linguaggio chiaro e semplice: le informazioni devono essere fornite nel modo più semplice possibile, concise e definitive per evitare margini di interpretazione. È possibile utilizzare altri mezzi oltre alla forma scritta. Si raccomanda di utilizzare dichiarazioni/informative privacy stratificate, che consentano ai visitatori del sito web di accedere a specifici aspetti rilevanti per loro. I metodi scelti per fornire le informazioni devono essere adeguati alle circostanze e alle informazioni da fornire. Il Richiedente è tenuto a fornire le informazioni agli interessati e alle parti interessate almeno nella lingua dello Stato membro in cui viene rilasciata la certificazione.	Interfaccia utente e materiale informativo fornito agli interessati. Clausole contrattuali (se applicabili).	12.1
G.3.1.2	C	G	A	Obbligo di facilitare l'esercizio dei diritti dell'interessato	A) Il Richiedente deve: a.1) informare gli interessati sulle modalità di esercizio dei loro diritti sul sito web del Richiedente; a.2) (E) disporre di personale addestrato a gestire le richieste degli interessati.	Il Richiedente deve facilitare l'esercizio dei diritti dell'interessato. Il Titolare del trattamento non può rifiutarsi di dare seguito alla richiesta dell'interessato di esercitare i diritti di cui agli articoli da 15 a 22, a meno che il Titolare del trattamento non dimostri di non essere in grado di identificare l'interessato.	Informazioni fornite agli interessati, anche sul sito web.	12.2

G.3.1.3	C	G	A	Garantire una corretta gestione e registrazione dei diritti degli interessati	A) Il Richiedente deve disporre di una procedura o di un meccanismo per: a.1) ricevere e registrare tutte le richieste degli interessati; a.2) (E) identificare e autenticare gli interessati in caso di incertezza sulla loro reale identità; a.3) (E) valutare e verificare che tutte le condizioni siano soddisfatte per procedere con la richiesta; a.4) (E) soddisfare la richiesta; a.5) (E) controllare il tempo che intercorre tra la ricezione della richiesta dell'interessato e la risposta e/o azione da parte del Richiedente. E B) Il Richiedente dovrà tenere un registro delle: b.1) richieste dell'interessato con la data di ricezione; b.2) (E) comunicazioni con gli interessati con le relative date; b.3) (E) azioni di follow-up con le relative date. b.4) (E) se del caso, delle ragioni del mancato rispetto della richiesta ricevuta.	Una chiara procedura scritta o una soluzione tecnologica deve garantire che ogni volta che un interessato comunica una richiesta al Richiedente, questa venga registrata ed processata senza ritardi ingiustificati. L'Auditor deve essere in grado di eseguire un test come se fosse un soggetto interessato. Deve essere in grado di reperire le informazioni su come presentare una richiesta e di eseguire una richiesta fittizia per controllare come la richiesta viene registrata e seguita.	Procedura o meccanismo in atto per la gestione delle richieste degli interessati. Se disponibili, registri di precedenti richieste di dati personali.	12.2
G.3.1.4	C	G	A	Informazioni senza ritardi ingiustificati	A) Il Richiedente deve dimostrare che la procedura o il meccanismo in atto sono efficaci e appropriati per: a.1) registrare le richieste di informazioni ricevute dagli interessati; a.2) (E) rispondere alle richieste ricevute entro e non oltre 30 giorni.	Il Richiedente deve tenere una registrazione sistematica delle: - richieste ricevute dagli interessati, compresa la data di ricezione; - comunicazione di follow-up con gli interessati, compresa la data della comunicazione; - azioni intraprese per dare seguito alle richieste ricevute, compresa la data dell'azione; - se del caso, delle ragioni del mancato rispetto della richiesta ricevuta. Il periodo di 30 giorni di cui al punto a.2 può essere prorogato di altri due mesi se necessario, tenendo conto della complessità e del numero delle richieste. Il Titolare del trattamento informerà l'interessato di tale proroga entro un mese dal ricevimento della richiesta, indicando i motivi del ritardo.	Procedura o meccanismo in atto per la gestione delle richieste degli interessati. Se disponibile, analisi a campione dei registri delle richieste degli interessati.	12.3
G.3.1.5	C	G	A	Risposta elettronica	A) Il Richiedente deve disporre di regole, procedure o un meccanismo per garantire che, quando l'interessato presenta la richiesta per via elettronica, le informazioni siano fornite di default anche per via elettronica.	Il Richiedente deve disporre di procedure o meccanismi per: - consentire agli interessati di presentare le loro richieste per via elettronica; - rispondere/adempiere alle richieste degli interessati con mezzi elettronici; - rispondere/adempiere alle richieste dell'interessato nel formato richiesto da quest'ultimo.	Interfaccia utente. Procedura o meccanismo in atto per la gestione delle richieste degli interessati.	12.3
G.3.1.6	C	G	A	Obbligo di informare e giustificare la mancata azione	A) Il Richiedente deve avere regole, procedure o un meccanismo in atto per informare e giustificare la mancata azione agli interessati. E B) Quando il Richiedente decide di non dare seguito a una richiesta di informazioni da parte di un interessato, lo informerà entro e non oltre 30 giorni dal ricevimento della richiesta: b.1) delle ragioni del mancato intervento; b.2) (E) della possibilità di presentare un reclamo ad un'Autorità di Controllo e della possibilità di ricorrere a un rimedio giudiziario.	Qualora il Titolare del trattamento nutra ragionevoli dubbi sull'identità della persona fisica che presenta la richiesta di cui agli articoli da 15 a 21, il Titolare del trattamento dovrebbe richiedere la fornitura di informazioni aggiuntive necessarie per confermare l'identità dell'interessato.	Procedura o meccanismo in atto per la gestione delle richieste degli interessati. Se disponibile, analisi a campione dei registri delle richieste degli interessati.	12.4. 12.6

G.3.1.7	C	G	A	Gratuito	A) Per impostazione predefinita, il Richiedente non addebiterà alcun costo agli interessati per informarli o per comunicare con loro nel contesto di una richiesta di esercizio dei loro diritti. E B) SE il Richiedente intende addebitare agli interessati i costi delle richieste non giustificate o eccessive, ALLORA deve disporre di una procedura scritta per: b.1) valutare in base a criteri fattuali se le richieste sono ragionevoli o eccessive; b.2) (E) documentare con motivazioni concrete qualsiasi decisione di non fornire informazioni gratuite; b.3) (E) valutare i costi amministrativi della relativa richiesta se ritenuti eccessivi; b.4) (E) proporre di addebitare all'interessato un costo ragionevole per soddisfare richieste manifestamente infondate o eccessive; b.5) (E) fornire una decisione motivata di non soddisfare la richiesta in modo gratuito.	Qualora le richieste di un interessato siano manifestamente infondate o eccessive, in in particolare a causa del loro carattere ripetitivo, il Titolare del trattamento può: (a) addebitare un costo ragionevole che tenga conto dei costi amministrativi per fornire l'informazione o la comunicazione o per intraprendere l'azione richiesta; oppure rifiutare di dare seguito alla richiesta.	Procedura o meccanismo in atto per la gestione delle richieste degli interessati. Se disponibile, analisi a campione dei registri delle richieste degli interessati.	12.5
G.3.1.8	C	G	A	Leggibilità delle icone da parte della macchina	SE il Richiedente utilizza le icone per informare gli interessati sulla propria policy di protezione dei dati attraverso mezzi elettronici ALLORA: A) Il Richiedente deve dimostrare che le sue icone utilizzate per informare gli interessati sulla sua policy di protezione dei dati personali sono leggibili a macchina.	Se il Richiedente utilizza icone per informare gli interessati sulla propria policy di protezione dei dati con mezzi elettronici, deve utilizzare icone leggibili a macchina. Ad esempio, è importante che gli interessati con disabilità, come la cecità, possano accedere alle informazioni fornite sull'interfaccia utente tramite applicazioni text-to-voice.	Policy di protezione dei dati comunicata sull'interfaccia utente. Se applicabile, test tecnico di leggibilità delle icone.	12.7
G.3.2				**Informazioni da fornire in caso di raccolta di dati personali presso l'interessato** Condizione: SE il Target of Evaluation tratta dati ottenuti direttamente dagli interessati, ALLORA: [Tranne nel caso in cui sia possibile dimostrare un'esenzione in conformità a G.3.2.3].				**13**
G.3.2.1	C	S	A	Obbligo di informazione	A) Le informazioni fornite all'interessato al momento della raccolta dei dati devono comprendere almeno le seguenti informazioni:	Il Richiedente ha l'obbligo di fornire informazioni chiare agli interessati quando raccoglie i loro dati personali.	Interfaccia utente o clausole contrattuali con l'interessato. Se disponibili, i registri delle informazioni trasmesse agli interessati.	13.1
				Dettagli del Titolare del trattamento	a.1) l'identità del Titolare del trattamento; a.2) (E) i dati di contatto del Titolare del trattamento;			13.1.a
				Contatto del DPO	a.3) (E) i dati di contatto del responsabile della protezione dei dati (o del meccanismo di contatto);			13.1.b
				Scopo	a.4) (E) le finalità del trattamento;			13.1.c
				Base giuridica	a.5) (E) la base giuridica del trattamento;			13.1.c
				Interessi legittimi	a.6) (E) se applicabile, i legittimi interessi perseguiti dal Titolare del trattamento o da una terza parte;			13.1.d
				Destinatari	a.7) (E) i destinatari o le categorie di destinatari dei dati personali;			13.1.e
				Trasferimento transfrontaliero	a.8) (E) se è probabile che i dati personali siano trasferiti in un paese terzo o ad una organizzazione internazionale, l'elenco dei Paesi extraeuropei in cui i dati vengono trasferiti; a.8) a.9) (E) se è probabile che i dati personali siano trasferiti in un paese terzo o ad una organizzazione internazionale, se si applica una decisione di adeguatezza valida al trasferimento dei dati; a.9) a.10) (E) se è probabile che i dati personali siano trasferiti in un paese terzo o ad una organizzazione internazionale, informazioni sulle misure di salvaguardia adottate dal Titolare del trattamento per valutare e ridurre al minimo i rischi per gli interessati e i loro diritti quando i dati vengono trattati in paesi terzi;			13.1.e
				Processo decisionale automatizzato	a.11) (E) se viene eseguito un processo decisionale automatizzato e/o la profilazione, informazioni significative sulla logica adottata nelle attività di trattamento; a.12) (E) se viene eseguito un processo decisionale automatizzato e/o la profilazione, la rilevanza delle attività di trattamento; a.13) (E) se viene eseguito un processo decisionale e/o di profilazione automatizzato, le conseguenze attese delle attività di trattamento;			13.2.f

				Periodo di conservazione	a.14) (E) il periodo di conservazione o i criteri per determinare il periodo di conservazione;			13.2.a
				Diritti dell'interessato	a.15) (E) informazioni sui diritti di accesso dell'interessato ai dati personali; a.16) (E) informazioni sui diritti dell'interessato alla rettifica dei dati personali; a.17) (E) informazioni sui diritti dell'interessato alla cancellazione dei dati personali; a.18) (E) informazioni sui diritti dell'interessato alla limitazione del trattamento dei dati; a.19) (E) informazioni sui diritti di opposizione dell'interessato al trattamento dei dati; a.20) (E) informazioni sui diritti dell'interessato alla portabilità dei dati;			13.2.b
				Diritto di revoca del consenso	a.21) (E) se il trattamento è basato sul consenso, il diritto di revocare il consenso in qualsiasi momento;			13.2.c
				Diritto di presentare un reclamo	a.22) (E) il diritto di presentare un reclamo all'Autorità di Controllo;			13.2.d
				Natura del requisito	a.23) (E) se la fornitura di dati personali è un requisito legale o contrattuale, o un requisito necessario per stipulare un contratto, nonché se l'interessato è obbligato a fornire i dati personali e le possibili conseguenze della mancata fornitura di tali dati.			13.2.e
G.3.2.2	C	S	A	Ulteriori trattamenti	A) Il Richiedente deve disporre di regole, procedure o meccanismi per informare gli interessati di qualsiasi ulteriore trattamento, anche per quanto riguarda la finalità del trattamento successivo e i diritti degli interessati. E B) Il Richiedente dovrà tenere un registro di: b.1) qualsiasi estensione del trattamento dei dati con le relative motivazioni; b.2) (E) la valutazione della liceità dell'ulteriore trattamento; b.3) (E) la comunicazione agli interessati (con le date).	Il Richiedente deve essere in grado di dimostrare l'efficacia della procedura tramite registri precedenti o dimostrazioni tecniche. Si noti che alcune informazioni potrebbero dover essere ulteriormente trattate in base alle leggi nazionali, come ad esempio gli obblighi post mortem.	Regole, procedure o meccanismi in atto per informare l'interessato di qualsiasi ulteriore trattamento.	13.3
G.3.2.3	C	S	E	Esenzione tollerata	Per derogare ai criteri G.3.2.1 e G.3.2.2, il Richiedente deve dimostrare che l'interessato è già stato informato.	Qualsiasi esenzione deve essere chiaramente giustificata e documentata.	Revisione della documentazione. Analisi del campione.	13.4

G.3.3				Informazioni da fornire quando i dati personali non sono stati ottenuti dall'interessato				14
				Condizione:	SE il Target of Evaluation tratta dati che non sono stati ottenuti dagli interessati, ALLORA: [Tranne nel caso in cui sia possibile dimostrare un'esenzione in conformità a G.3.3.4].			
G.3.3.1	C	S	A	Obbligo di informazione	A) L'informativa fornita all'interessato deve contenere le seguenti informazioni:	Il Richiedente deve conservare i registri delle informazioni ottenute dall'interessato ed essere in grado di dimostrare che l'interessato ha già accesso alle informazioni per essere esentato da questi criteri. Questi punti non devono essere applicati se e nella misura in cui l'interessato dispone già delle informazioni.	Interfaccia utente e materiale informativo fornito agli interessati. Clausole contrattuali (se applicabili).	14.1
				Dettagli del Titolare Dati di contatto del DPO	a.1) l'identità del Titolare del trattamento; a.2) (E) i dati di contatto del Titolare del trattamento;			14.1.a
					a.3) (E) i dati di contatto del responsabile della protezione dei dati (o del meccanismo di contatto);			14.1.b
				Finalità	a.4) (E) le finalità del trattamento;			14.1.c
				Base giuridica	a.5) (E) la base giuridica del trattamento;			14.1.c
				Interessi legittimi	a.6) (E) se applicabile, i legittimi interessi perseguiti dal Titolare del trattamento o da una terza parte;			14.2.b
				Categorie di dati	a.7) (E) le categorie di dati personali interessate;			14.1.d
					a.8) (E) i destinatari o le categorie di destinatari dei dati personali;			14.1.e
				Destinatari Trasferimento transfrontaliero	a.9) (E) se è probabile che i dati personali siano trasferiti in un paese terzo o ad una organizzazione internazionale, l'elenco dei Paesi extraeuropei in cui i dati sono trasferito; a.10) (E) se è probabile che i dati personali siano trasferiti in un paese terzo o ad una organizzazione internazionale, se al trasferimento dei dati si applica una decisione di adeguatezza valida; a.11) (E) se è probabile che i dati personali siano trasferiti in un paese terzo o ad una organizzazione internazionale, informazioni sulle misure di salvaguardia adottate dal Titolare del trattamento per valutare e ridurre al minimo i rischi per gli interessati e i loro diritti quando i dati vengono trattati in paesi terzi;			14.1.f
				Processo decisionale automatizzato	a.12) (E) se viene effettuato un processo decisionale e/o di profilazione automatizzato, informazioni significative sulla logica che ha caratterizzato le attività di trattamento; a.13) (E) se viene eseguito un processo decisionale e/o di profilazione automatizzato, la rilevanza delle attività di trattamento; a.14) (E) se viene effettuato un processo decisionale e/o di profilazione automatizzato, le conseguenze attese delle attività di trattamento;			14.2.g
				Periodo di conservazione Diritti dell'interessato	a.15) (E) il periodo di conservazione o i criteri per determinare il periodo di conservazione;			14.2.a
					a.16) (E) informazioni sui diritti di accesso dell'interessato ai dati personali; a.17) (E) informazioni sui diritti dell'interessato alla rettifica dei dati personali; a.18) (E) informazioni sui diritti dell'interessato alla cancellazione dei dati personali; a.19) (E) informazioni sui diritti dell'interessato alla limitazione del trattamento dei dati; a.20) (E) informazioni sui diritti di opposizione dell'interessato al trattamento dei dati; a.21) (E) informazioni sui diritti dell'interessato alla portabilità dei dati;			14.2.c
				Diritto di revoca del consenso	a.22) (E) se il trattamento è basato sul consenso, il diritto di revocare il consenso in qualsiasi momento;			14.2.d
				Diritto di presentare un reclamo	a.23) (E) il diritto di presentare un reclamo all'Autorità di Controllo;			14.2.e
				Fonte dei dati	a.24) (E) l'origine dei dati personali; a.25) (E) se applicabile, se le informazioni sono state raccolte da fonti applicabili al pubblico.			14.2.f

G.3.3.2	C	S	A	Obbligo di informare in tempo utile	A) Il Richiedente deve disporre di una procedura per informare gli interessati in merito alla raccolta indiretta dei loro dati. E B) Il Richiedente dovrà tenere un registro con: b.1) la data in cui i dati personali sono stati raccolti indirettamente; b.2) (E) la comunicazione agli interessati con le date; b.3) (E) le informazioni fornite agli interessati. E C) I registri devono dimostrare che il Titolare del trattamento ha fornito informazioni agli interessati: c.1) entro e non oltre 30 giorni; c.2) (E) se i dati personali devono essere utilizzati per comunicare con l'interessato, al momento della prima comunicazione agli interessati; c.3) (E) se è prevista la divulgazione a un altro destinatario, al più tardi al momento della prima divulgazione dei dati personali.	Una chiara procedura scritta o una soluzione tecnologica deve garantire che ogni volta che un soggetto interessato comunica una richiesta al Richiedente, questa venga registrata ed processata senza ritardi ingiustificati. L'Auditor deve essere in grado di eseguire un test come se fosse un soggetto interessato. Deve essere in grado di trovare le informazioni su come presentare una richiesta ed eseguire una richiesta fittizia per verificare come la richiesta viene registrata e seguita. A tempo debito: un periodo di tempo ragionevole dopo l'ottenimento dei dati personali, ma al più tardi entro un mese, tenuto conto delle circostanze specifiche in cui i dati personali sono trattati; o se i dati personali devono essere utilizzati per comunicare con l'interessato, al più tardi al momento della prima comunicazione a tale interessato; o se è prevista la divulgazione a un altro destinatario, al più tardi quando i dati personali sono divulgati per la prima volta.	Regole, procedure o meccanismi in atto per informare gli interessati. Se disponibili, i registri di precedenti comunicazioni con gli interessati.	14.3
G.3.3.3	C	S	A	Obbligo di informazione sull'estensione delle finalità	A) Il Richiedente deve disporre di una procedura per informare gli interessati su qualsiasi ulteriore trattamento dei loro dati personali previsto per finalità diverse da quelle dichiarate per cui i dati sono stati inizialmente raccolti. E B) Il Richiedente deve dimostrare l'efficacia della procedura.	Il Richiedente deve assicurarsi che le informazioni fornite siano in linea con l'art. 14 comma 2 del GDPR. 14, paragrafo 2.	Regole, procedure o meccanismi per informare gli interessati. Se disponibili, registri di precedenti comunicazioni con gli interessati sull'estensione della finalità.	14.4
G.3.3.4	C	S	E	Esenzione tollerata	SE si verifica uno dei seguenti casi, ALLORA G.3.3.1 può essere saltato:	Qualsiasi esenzione deve essere chiaramente giustificata e documentata. Anche se il regolamento può autorizzare alcune esenzioni, Europrivacy incoraggia i richiedenti a rispettare l'obbligo regolare.	DPO, interfaccia utente, comunicazione con gli interessati, leggi in materia.	14.5
				Precedente informazioni	Caso 1 - Già informati: A) Il Richiedente dovrà dimostrare che gli interessati sono già in possesso delle informazioni elencate in G.3.3.1.			14.5.a
				Sforzo sproporzionato	O Caso 2 - Impossibile o sproporzionato: A) Il Richiedente deve dimostrare che la fornitura di tali informazioni: a.1) si rivela impossibile; a.2) (OP) comporterebbe uno sforzo sproporzionato; a.3) (OPPURE) rischia di rendere impossibile o di pregiudicare gravemente il raggiungimento degli obiettivi di tale trattamento. E B) Il Titolare del trattamento deve aver adottato misure adeguate per tutelare i diritti, le libertà e gli interessi dell'interessato, anche rendendo pubbliche le informazioni.			14.5.b
				Obbligo legale	O Caso 3 - Base giuridica: A) Il Richiedente deve dimostrare di essere vincolato da uno specifico obbligo legale che richiede espressamente l'ottenimento o la divulgazione di dati personali.			14.5.c
				Segreto professionale regolamentato	O Caso 4 - Segretezza: A) Il Richiedente deve dimostrare di essere soggetto a un obbligo di segretezza regolato dalla legge, incluso un obbligo statutario di segretezza.			14.5.d

G.3.4				Diritto di accesso dell'interessato				15
G.3.4.1	C	S	A	Diritto di accesso dell'interessato	A) Il Richiedente deve disporre di un meccanismo o di una procedura efficace che consenta agli interessati di richiedere e accedere alle seguenti informazioni:	Il Richiedente deve disporre di un meccanismo o di una procedura efficace che consenta agli interessati di richiedere e accedere alle informazioni sul trattamento dei dati. Il Richiedente deve garantire che il trattamento dei dati sia conforme alle normative nazionali applicabili.	Procedura o meccanismo in atto per la gestione delle richieste degli interessati. Se disponibili, i registri delle richieste precedenti e delle azioni di follow-up sul diritto di accesso.	15.1
				Finalità	a.1) le finalità del trattamento;			15.1.a
				Categorie di dati	a.2) (E) le categorie di dati personali trattati;			15.1.b
				Destinatari	a.3) (E) i destinatari o le categorie di destinatari;			15.1.c
				Periodo di conservazione	a.4) (E) il periodo di conservazione o i criteri per determinare il periodo di conservazione;			15.1.d
				Diritti degli interessati	a.5) (E) informazioni sui diritti dell'interessato ad accedere ai propri dati; a.6) (E) informazioni sui diritti di rettifica dell'interessato; a.7) (E) informazioni sui diritti dell'interessato alla cancellazione dei dati personali; a.8) (E) informazioni sui diritti dell'interessato alla limitazione del trattamento; a.9) (E) informazioni sui diritti di opposizione dell'interessato; a.10) (E) informazioni sui diritti dell'interessato alla portabilità dei dati;			15.1.e
				Diritto di presentare un reclamo	a.11) (E) il diritto di presentare un reclamo all'Autorità di Contrp;;p;			15.1.f
				Fonte dei dati	a.12) (E) la fonte da cui provengono i dati personali e, se del caso, se i dati personali provengono da una fonte pubblica;			15.1.g
				Processo decisionale automatizzato	a.13) (E) se il Titolare del trattamento ha attuato un processo decisionale automatizzato e di profilazione; a.14) (E) se il Titolare del trattamento ha attuato un processo decisionale automatizzato o la profilazione, informazioni significative sulla logica adottata nelle attività di trattamento; a.15) (E) se il Titolare del trattamento ha attuato un processo decisionale o di profilazione automatizzato, la rilevanza delle attività di trattamento; a.16) (E) se il Titolare ha attuato un processo decisionale automatizzato o la profilazione, le conseguenze attese delle attività di trattamento;			15.1.h
				Trasferimento transfrontaliero	a.17) (E) se i dati personali sono trasferiti a un paese terzo o ad una organizzazione internazionale; a.18) (E) se i dati personali sono trasferiti a un paese terzo o ad una organizzazione internazionale, l'elenco dei paesi terzi in cui i dati sono trasferiti; a.19) (E) se i dati personali sono trasferiti a un paese terzo o ad una organizzazione internazionale, se al trasferimento dei dati si applica una decisione di adeguatezza valida; a.20) (E) se i dati personali sono trasferiti a un paese terzo o ad una organizzazione internazionale, informazioni sulle misure di salvaguardia adottate dal Titolare del trattamento per valutare e ridurre al minimo i rischi per gli interessati e i loro diritti in caso di trattamento in paesi terzi.			15.2
G.3.4.2	C	S	A	Obbligo di fornire una copia	A) I dati personali trattati nell'ambito del Target of Evaluation devono essere estraibili e trasferibili all'Interessato che ne ha fatto richiesta in un formato elettronico di uso comune.	Il diritto alla portabilità è un diritto fondamentale. Per facilitare il processo, il Richiedente può decidere di consentire agli interessati di accedere e scaricare i propri dati personali da soli. Per ogni ulteriore copia richiesta dall'interessato, il Titolare del trattamento può addebitare un costo ragionevole basato sui costi amministrativi.	Procedura o meccanismo in atto per trasferire copie dei dati agli interessati. Se disponibili, i registri di precedenti comunicazioni con gli interessati.	15.3

G.3.4.3	C	S	A	Dovere di proteggere i diritti degli altri	A) Il Richiedente deve disporre di una procedura o di un meccanismo per evitare effetti negativi sui diritti e sulle libertà di altri interessati quando soddisfa la richiesta di un interessato del trasferimento di una copia dei propri dati personali.	Se del caso, il Richiedente deve cancellare i dati personali di altri interessati che potrebbero essere impattati dall'esercizio del diritto o deve richiedere il loro consenso prima di fornire la copia.	Regole, procedure o meccanismi in atto per trasferire copie dei dati agli interessati. Se disponibili, i registri di precedenti comunicazioni con gli interessati.	15.4
G.3.5				**Diritto di rettifica**				**16**
G.3.5.1	C	S	A	Diritto di rettifica	A) Il Richiedente deve dimostrare che la procedura o il meccanismo in atto per ottemperare al diritto dell'interessato di rettificare o completare i propri dati personali consente di implementare efficacemente la richiesta.	Il Richiedente deve tenere un registro: - delle richieste degli interessati con le relative date; - delle comunicazioni con gli interessati con la/e data/e; - della/e azione/i di follow-up con la/e data/e; - se del caso, delle ragioni del mancato rispetto della richiesta ricevuta. L'effettiva attuazione di questo requisito richiede che la procedura o il meccanismo in atto siano testati dall'Auditor o valutati attraverso un'analisi a campione delle richieste degli interessati.	Regole, procedure o meccanismi in atto per la rettifica dei dati. Se disponibili, registri di precedenti richieste e azioni di follow-up sul diritto alla rettifica.	16
G.3.6				**Diritto alla cancellazione ("diritto all'oblio")**				**17**
G.3.6.1	C	S	A	Diritto alla cancellazione	A) Il Richiedente deve disporre di regole, procedure o meccanismi per cancellare efficacemente i dati personali che non sono più necessari (in relazione alla finalità per cui sono stati raccolti o trattati).	Il Richiedente deve disporre di una procedura per: - registrare la richiesta dell'interessato; - identificare e autenticare l'interessato in caso di incertezza sulla sua identità; - eseguire la cancellazione dei dati personali richiesta. Il Richiedente deve tenere un registro: - delle richieste degli interessati con le relative date; - delle comunicazioni con gli interessati con la/e data/e; - della/e azione/i di follow-up con la/e data/e; - della valutazione delle condizioni per l'adempimento della richiesta (dati non più necessari; revoca del consenso; opposizione dell'interessato; trattamento illecito; adempimento di obblighi di legge; o offerta di servizi della società dell'informazione a minori di età); - se del caso, delle ragioni del mancato rispetto della richiesta ricevuta. L'efficacia deve essere dimostrata testando la procedura o analizzando le precedenti richieste degli interessati e verificando che i dati siano effettivamente cancellati.	Regole, procedure o meccanismi in atto per la cancellazione dei dati. Se disponibili, registri di precedenti richieste e azioni di follow-up sul diritto alla cancellazione.	17.1
G.3.6.2	C	S	A	Obbligo di trasmettere la richiesta ad altri responsabili del trattamento dei dati	SE il Richiedente ha reso pubblici i dati personali del Target of Evaluation ad altri responsabili del trattamento, ALLORA: A) Il Richiedente deve disporre di regole, di una procedura o di un meccanismo per informare gli altri Titolari del trattamento della richiesta di cancellazione da parte degli interessati, tranne nel caso in cui il Richiedente abbia valutato le potenziali misure per informare gli altri Titolari del trattamento e ha dimostrato che le misure individuate sarebbero state sproporzionate.	Il Titolare del trattamento, tenendo conto della tecnologia disponibile e dei costi di attuazione, deve adottare misure ragionevoli, anche tecniche, per informare i Titolari del trattamento che trattano i dati personali che l'interessato ha richiesto la cancellazione da parte di tali Titolari di qualsiasi collegamento, copia o riproduzione di tali dati personali.	Regole, procedure o meccanismi in atto per il trasferimento dei dati ad altri Titolari del trattamento. Se disponibili, registri di precedenti richieste e azioni di follow-up per il trasferimento dei dati.	*17.2*
G.3.6.3	C	S	E	Esenzione tollerata	Il diritto alla cancellazione è soggetto a restrizioni nei seguenti casi: *Esercizio del diritto alla libertà di espressione e di informazione:* A) Le prove devono dimostrare che i dati conservati sono utilizzati nell'ambito di un servizio di pubblica informazione o espressione. *(OR) Obbligo legale:* A) Le prove devono dimostrare che il Richiedente è vincolato dall'obbligo di adempiere a tale obbligo legale.	Qualsiasi esenzione deve essere chiaramente giustificata e documentata. Anche se il GDPR autorizza alcune esenzioni, Europrivacy incoraggia i Richiedenti a rispettare l'obbligo regolare.	Registri e interviste del DPO, informativa sulla privacy, prove raccolte.	17.3 17.3.a 17.3.b

				(OR) Interesse pubblico: A) Le prove devono dimostrare l'esistenza di un interesse pubblico nel settore della salute pubblica.			17.3.c
				(OR) Archiviazione, ricerca o statistica: A) Le prove devono dimostrare che la conservazione dei dati è collegata a: a.1) finalità di archiviazione nel pubblico interesse; a.2) (OPPURE) scopi scientifici; a.3) (OPPURE) scopi di ricerca storica; a.4) (OPPURE) fini statistici.			17.3.d
				(OR) Procedura legale: A) Le prove devono dimostrare che la conservazione dei dati è legata all'accertamento, all'esercizio o alla difesa di diritti legali.			17.3.e
G.3.7				**Diritto alla limitazione del trattamento**				**18**
G.3.7.1	C	S	A	Diritto alla limitazione del trattamento	A) Il Richiedente deve disporre di regole, di una procedura o di un meccanismo atto a: a.1) soddisfare efficacemente le richieste degli interessati di limitare il trattamento dei loro dati personali; a.2) (E) garantire che i trattamenti di dati personali il cui trattamento è limitato possano solo essere effettuati: - con il consenso dell'interessato; - per l'accertamento, l'esercizio o la difesa di diritti legali; - per proteggere i diritti di un'altra persona fisica o giuridica; - per motivi di rilevante interesse pubblico; a.3) (E) per documentare le decisioni di revoca delle restrizioni al trattamento dei dati; a.4) (E) garantire che l'interessato sia informato prima di revocare la restrizione al trattamento dei suoi dati personali.	Per quanto riguarda la limitazione dei dati, il Richiedente deve garantire che le operazioni di trattamento che sono state limitate su richiesta degli interessati tornino ad essere pienamente efficaci solo dopo che l'interessato ha dato il suo consenso ed è stato informato della revoca della limitazione. Dovrebbe essere necessario garantire che l'interessato abbia prestato il proprio consenso alle condizioni di liceità sopra indicate, ma anche che il Titolare del trattamento abbia conservato la documentazione e la prova del consenso.	Regole, procedure o meccanismi per limitare il trattamento dei dati. Se disponibili, i registri delle richieste precedenti e le azioni di follow-up per la restrizione.	18.1
G.3.8				**Obbligo di notifica in merito alla rettifica o alla cancellazione dei dati personali o alla limitazione del trattamento**				**19**
G.3.8.1	C	S	A	Obbligo di informare i destinatari	A) Il Richiedente deve disporre di una procedura o di un meccanismo per comunicare ogni rettifica o cancellazione dei dati personali o la limitazione del trattamento effettuato nei confronti di ciascun destinatario a cui sono stati comunicati i dati personali. O B) Il Richiedente dovrà dimostrare che l'obbligo di informare il destinatario è impossibile o comporta uno sforzo sproporzionato.	Il Richiedente deve tenere un registro con: - la comunicazione effettuata per informare i destinatari dei dati con data e ora; - se del caso, le motivazioni per cui i destinatari non sono stati informati.	Regole, procedure o meccanismi in atto per notificare rettifiche e cancellazioni. Se disponibili, i registri delle notifiche precedenti.	19
G.3.8.2	C	S	A	Obbligo di informare gli interessati sui destinatari, se richiesto.	A) Il Richiedente deve disporre di regole, procedure o meccanismi per soddisfare efficacemente le richieste degli interessati di essere informati sui destinatari dei loro dati personali.	Il Richiedente può disporre di una procedura o di un meccanismo per: - registrare la richiesta dell'interessato; - identificare e autenticare l'interessato in caso di incertezza sulla sua identità; - valutare e verificare che tutte le condizioni siano soddisfatte per procedere con la richiesta; - informare l'interessato sui destinatari come richiesto Il Richiedente deve tenere un registro delle: - richieste degli interessati e le relative date; - comunicazioni con gli interessati con la/e data/e; - delle valutazioni delle richieste e la/e azione/i di follow-up con la/e data/e; - se del caso, delle ragioni del mancato rispetto della richiesta ricevuta.	Regole, procedure o meccanismi in atto per rispondere alle richieste degli interessati. Se disponibili, registri di precedenti informazioni fornite agli interessati.	19

G.3.9				**Diritto alla portabilità dei dati**				**20**
				Condizione:	SE i dati personali sono raccolti con il consenso o attraverso un contratto con gli interessati, ALLORA:			
G.3.9.1	C	S	A	Diritto alla portabilità dei dati	A) Il Richiedente deve disporre di una procedura o di un meccanismo per la portabilità dei dati che: a.1) deve consentire agli interessati di ottenere una copia dei dati personali forniti in formato elettronico; a.2) (E) deve filtrare i dati personali relativi ad altri interessati se questo può incidere negativamente sui diritti e sulla libertà di questi ultimi; E B) Il formato dei dati utilizzato per trasferire i dati personali all'interessato sarà: b.1) strutturato; b.2) (E) di uso comune; b.3) (E) leggibile a macchina.	Ove tecnicamente possibile, il Richiedente può consentire all'interessato di accedere direttamente ai propri dati trattati. Il Richiedente può disporre di una procedura o di un meccanismo per: - registrare la richiesta dell'interessato; - identificare e autenticare l'interessato in caso di incertezza sulla sua identità; - valutare e verificare che tutte le condizioni siano soddisfatte per procedere con la richiesta; - trasmettere i dati richiesti all'interessato. Il Richiedente deve tenere un registro delle: - richieste degli interessati con le relative date; - comunicazioni con gli interessati con la/e data/e; - la valutazione della richiesta e la/e azione/i di follow-up con la/e data/e; - se del caso, le ragioni del mancato rispetto della richiesta ricevuta. Il Richiedente deve dimostrare (estratto dei registri passati o dimostrazione tecnica) che la procedura è adeguata per rispondere efficacemente alla richiesta dell'interessato. L'applicazione di questo diritto dovrebbe avvenire senza ostacoli da parte del Titolare del trattamento a cui sono stati forniti i dati personali, qualora il trattamento sia basato sul consenso o su un contratto, o il trattamento sia effettuato con mezzi automatizzati.	Regole, procedure o meccanismi in vigore per la portabilità dei dati. Test tecnico o dimostrazione della portabilità dei dati.	20.1
G.3.10				**Diritto di opposizione**				**21**
G.3.10.1	C	S	A	Efficacia del diritto di opposizione	A) Il Richiedente deve disporre di regole, procedure o meccanismi per soddisfare efficacemente le richieste di opposizione al trattamento dei propri dati personali da parte degli interessati.	Il Richiedente può disporre di una procedura per: - registrare la richiesta dell'interessato; - identificare e autenticare l'interessato in caso di incertezza sulla sua identità; - valutare e verificare che tutte le condizioni siano soddisfatte per procedere con la richiesta; - interrompere il trattamento come richiesto dall'interessato senza ritardi ingiustificati. Il Richiedente deve tenere un registro delle: - richieste degli interessati con le relative date; - comunicazioni con gli interessati con la/e data/e; - valutazioni delle richieste e la/e azione/i di follow-up con la/e data/e; - se del caso, delle ragioni del mancato rispetto della richiesta ricevuta.	Regole, procedure o meccanismi per affrontare il diritto all'obiezione. Se disponibili, registri di precedenti richieste e azioni di follow-up sul diritto di opposizione.	21
G.3.10.2	C	S	A	Informazioni chiare sul diritto di opposizione	A) Il Richiedente deve informare gli interessati del loro diritto di opporsi al trattamento dei loro dati personali: a.1) prima di trattare i loro dati; a.2) (E) in un paragrafo distinto.	Il Richiedente deve tenere traccia delle informazioni fornite all'interessato, dimostrando come il diritto di opposizione sia stato esplicitamente portato a conoscenza dell'interessato.	Interfaccia utente e materiale informativo fornito agli interessati. Clausole contrattuali (se applicabili).	21.4

G.3.11				**Diritto a non essere sottoposti a un processo decisionale individuale automatizzato, compresa la profilazione**				**22**
G.3.11.1	C	S	A	Processo decisionale individuale automatizzato, compresa la profilazione	A) Il trattamento dei dati nell'ambito del Target of Evaluation è esente da decisioni basate esclusivamente su decisioni automatizzate che possono avere effetti sugli interessati, tranne nel caso in cui il processo decisionale automatizzato soddisfi almeno una delle seguenti condizioni: a.1) la necessità del trattamento per la stipula o l'esecuzione di un contratto tra l'interessato e il Titolare del trattamento è giustificata da un'analisi scritta del processo che deve aver preso in considerazione alternative al processo decisionale automatizzato per raggiungere un risultato equivalente e deve concludere che il processo decisionale automatizzato è necessario; a.2) (OPPURE) il trattamento è autorizzato dalla legge a cui è soggetto il Titolare; a.3) (OPPURE) il trattamento si basa sul consenso esplicito dell'interessato.	SE viene eseguito un trattamento automatizzato, il Richiedente deve documentare e dimostrare che: - il DPO ha valutato i rischi del previsto trattamento automatizzato dei dati per le libertà e i diritti degli interessati; - il DPO ha valutato e convalidato la liceità e la conformità del trattamento dei dati con il Diritto di non essere oggetto di un processo decisionale individuale automatizzato, compresa la profilazione; - la giustificazione e, se del caso, le misure tecniche e organizzative complementari da attuare per salvaguardare le libertà e i diritti degli interessati. Il Richiedente deve consentire a auditor esterni di valutare la conformità di questo trattamento dei dati con il diritto di cui sopra attraverso ispezioni, test o revisione della documentazione. La necessità deve essere dimostrata attraverso un'analisi del processo, prendendo in considerazione le alternative al processo decisionale automatizzato per raggiungere un risultato equivalente. Se esiste una soluzione equivalente che non richiede il trattamento automatizzato dei dati e fornisce gli stessi risultati, il processo decisionale automatizzato deve essere considerato non necessario.	Regole, policy e procedure interne. Registri delle comunicazioni con gli interessati. Interviste dei dipendenti. Ispezione e analisi del trattamento dei dati.	22.1
G.3.11.2	C	S	A	Diritti di ottenere l'intervento umano e d i contestare	SE le decisioni automatizzate si basano sul trattamento dei dati personali, ALLORA: A) Il Richiedente deve disporre di una procedura o di un meccanismo che permetta agli interessati: a.1) di ottenere l'intervento umano da parte del Titolare del trattamento; a.2) (E) di esprimere il proprio punto di vista e contestare la decisione.	Qualsiasi esenzione deve essere chiaramente giustificata e documentata. Ciò richiede che la procedura o il meccanismo in atto siano testati dall'auditor o valutati attraverso un'analisi a campione delle richieste degli interessati.	Procedura o meccanismo in atto per ottenere l'intervento umano. Informazioni fornite all'interessato. Se applicabile, le clausole contrattuali.	22.3
G.4				**Responsabilità del Titolare del trattamento** Obiettivo: Garantire che il Titolare del trattamento si attenga alla sua responsabilità normativa per il trattamento dei dati nell'ambito del Target of Evaluation. Condizione: SE il Richiedente è un Titolare del trattamento, ALLORA:				
G.4.1				**Responsabilità del Titolare del trattamento**				**24**
G.4.1.1	C	S	A	Documentazione sulle misure tecniche e organizzative	A) Il Richiedente deve disporre di una documentazione scritta delle misure tecniche e organizzative adottate per la protezione dei dati trattati.		Documentazione sulle misure tecniche e organizzative.	24.1
G.4.1.2	C	S	A	Obbligo di revisione e aggiornamento	A) Il Richiedente deve disporre di una procedura per rivedere periodicamente (almeno annualmente) l'adeguatezza delle misure tecniche e organizzative adottate. E B) Il Richiedente deve tenere traccia nei registri: b.1) della revisione delle misure tecniche e organizzative; b.2) delle vulnerabilità identificate e delle azioni intraprese per affrontarle.	SE il trattamento dei dati nell'ambito del Target of Evaluation comprende categorie particolari di dati, o è specificamente destinato a minori di età, o può esporre gli interessati a rischi per le libertà e i diritti: - L'audit interno e/o esterno sulla protezione dei dati deve essere effettuato almeno una volta ogni 12 mesi; - La revisione della policy di protezione dei dati da parte del DPO e/o del top management deve essere effettuata almeno ogni 12 mesi.	Regole, policy e procedure interne. Documentazione dell'ultima revisione delle misure tecniche e organizzative. Interviste dei dipendenti e del DPO.	24.1

G.4.1.3	C	S	A	Policies di protezione dei dati	A) Il Richiedente deve disporre di regole e/o policy scritte di protezione dei dati che comprendano almeno: a.1) sicurezza e controllo degli accessi; a.2) (E) gestione della violazione dei dati personali; a.3) (E) valutazione del rischio e, se del caso, valutazione d'impatto sulla protezione dei dati (DPIA); a.4) (E) requisiti e valutazione della conformità dei Responsabili del trattamento; a.5) (E) procedura di informazione e collaborazione con l'Autorità di Controllo; a.6) (E) policy di protezione dei dati by design e by default, come la minimizzazione dei dati e la pseudonimizzazione dei dati; a.7) (E) gestione del trasferimento dei dati a terzi e a paesi terzi.	Il Richiedente deve avere regole e/o policy scritte sulla protezione dei dati.	Norme e policy di protezione dei dati.	24.2
G.5				**Responsabili del trattamento (o sub-responsabili del trattamento)** Obiettivo: Garantire che i Responsabili del trattamento che partecipano al trattamento dei dati del Target of Evaluation rispettino i requisiti normativi. Condizione: SE i Responsabili o i sub-responsabili del trattamento sono coinvolti nel Target of Evaluation ALLORA:				
G.5.1				**Responsabili del Trattamento**				**28**
G.5.1.1	CP	S	A	Restrizione all'uso dei Responsabili del trattamento	A) Il Richiedente deve avere regole, una procedura o un meccanismo per: a.1) richiedere e registrare informazioni nei confronti dei propri Responsabili del trattamento in merito alle loro misure tecniche e organizzative per la protezione dei dati personali e/o certificazioni relative al GDPR; a.2) (E) valutare l'adeguatezza delle misure tecniche e organizzative segnalate dal Responsabile del trattamento per la protezione dei dati personali; a.3) (E) documentare e registrare la decisione di accettare i servizi del Responsabile del trattamento. E B) Il Richiedente deve tenere registri documentati: b.1) delle informazioni e delle garanzie fornite dal Responsabile del trattamento sulle sue Misure Tecniche e Organizzative; b.2) (E) il processo di valutazione e decisione di accettare i Responsabili del trattamento dei dati coinvolti nel trattamento dei dati del Target of Evaluation. E C) Il Richiedente deve disporre di regole o di una procedura per effettuare una revisione periodica delle clausole contrattuali e delle garanzie fornite dai suoi responsabili del trattamento che dimostrino l'adeguatezza delle sue misure tecniche e organizzative.	Il Richiedente deve disporre di regole, di una procedura o di un meccanismo per valutare e documentare la conformità del Responsabile del trattamento con i requisiti di protezione dei dati personali. Il Richiedente è tenuto a riesaminare periodicamente le clausole contrattuali e le garanzie fornite dai propri responsabili del trattamento per dimostrare l'adeguatezza delle proprie misure tecniche e organizzative. L'adeguatezza si riferisce alla capacità delle misure tecniche e organizzative di proteggere i diritti e le libertà degli interessati.	Regole, procedure o meccanismi in atto per valutare la conformità dei Responsabili del trattamento. Registri e documentazione delle precedenti valutazioni dei Responsabili del trattamento.	28.1
G.5.1.2	C	S	A	Necessità contrattuale per i controllori	A) Il Richiedente deve avere un rapporto contrattuale scritto con ogni singolo Responsabile del trattamento che si occupa di trattare dati nell'ambito del Target of Evaluation che dovrà: a.1) essere ammissibile a un tribunale di uno Stato membro dell'Unione europea; a.2) (E) specificare l'oggetto e la durata del trattamento; a.3) (E) specificare la natura e le finalità del trattamento; a.4) (E) specificare il tipo di dati personali; a.5) (E) specificare le categorie di interessati; a.6) (E) specificare i diritti e gli obblighi del Titolare del trattamento.	Il Titolare e il Responsabile del trattamento devono avere un rapporto contrattuale scritto, che deve essere conforme all'articolo 28 del GDPR.	Contratti del Titolare del trattamento con i Responsabili del trattamento.	28.3

G.5.1.3	P	S	A	Necessità contrattuale per i Responsabili del trattamento	SE il Richiedente agisce come Responsabile del trattamento, ALLORA: A) Il Richiedente deve regolare i suoi rapporti contrattuali in forma scritta con ogni singolo Titolare e Sub-Responsabile del trattamento dei dati nell'ambito del Target of Evaluation. E B) Ogni rapporto contrattuale con i Titolari e i Sub-Responsabili del trattamento dei dati coinvolti nel Target of Evaluation dovrà: b.1) essere ammissibile a un tribunale di uno Stato membro dell'Unione europea; b.2) (E) specificare l'oggetto e la durata del trattamento; b.3) (E) specificare la natura e le finalità del trattamento; b.4) (E) specificare il tipo di dati personali; b.5) (E) specificare le categorie di interessati; b.6) (E) specificare i diritti e gli obblighi del Titolare del trattamento.	Il Titolare del trattamento e il Responsabile del trattamento devono avere un rapporto contrattuale scritto, che deve essere conforme all'articolo 28 del GDPR.	Contratti del Responsabile del trattamento con i Responsabili del trattamento e i Sub-Responsabili.	28.3
G.5.1.4	CP	S	A	Obblighi contrattuali dei Responsabili del trattamento	A) Il rapporto contrattuale con ciascuno dei Responsabili del trattamento dei dati coinvolti nel Target of Evaluation stabilisce che il Responsabile deve: a.1) trattare i dati personali solo su istruzioni documentate del Titolare; a.2) (E) garantire che tutti coloro che sono autorizzati a trattare i dati personali nell'ambito del Target of Evaluation siano vincolati da obblighi di riservatezza; a.3) (E) attuare tutte le misure richieste ai sensi della Sicurezza del trattamento; a.4) (E) impegnarsi a non incaricare altri Responsabili del trattamento (o Sub-Responsabili del trattamento) senza accordo con il Titolare del trattamento; a.5) (E) adempiere all'obbligo di rispondere alle richieste degli interessati; a.6) (E) assistere il Titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, per l'adempimento dell'obbligo del Titolare del trattamento di rispondere a richieste di esercizio dei diritti dell'interessato; a.7) (E) assistere il Titolare del trattamento nel garantire l'osservanza degli obblighi in materia di sicurezza del trattamento dei dati, come la valutazione del rischio, la gestione e la notifica delle violazioni dei dati personali, la valutazione dell'impatto sulla protezione dei dati e la consultazione preventiva con l'autorità; a.8) (E) a scelta del Titolare del trattamento, cancellare o restituire tutti i dati personali al Titolare del trattamento dopo la fine della fornitura dei servizi relativi al trattamento, e cancella le copie esistenti, a meno che non sia diversamente disposto dalla legge; a.9) (E) mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie a dimostrare la conformità al regolamento; a.10) (E) autorizzare le ispezioni condotte dal Titolare del trattamento o da un altro auditor incaricato dal Titolare del trattamento; a.11) (E) richiedere che ai Sub-Responsabili del trattamento siano richiesti gli stessi obblighi e le stesse tutele che il Responsabile del trattamento contrae per l'esecuzione di specifiche attività di trattamento per conto del Titolare del trattamento.	Il Titolare e il Responsabile del trattamento devono avere un rapporto contrattuale scritto, che deve essere conforme ai requisiti di cui all'articolo 28 del GDPR. I Responsabili del trattamento devono garantire un'adeguata sicurezza e protezione dei dati trattati in linea con gli artt. 32-36 del GDPR.	Clausole contrattuali.	28.3
G.5.1.5	CP	S	A	Dimostrazione complementare della conformità dei Responsabili del trattamento	A) Il Richiedente deve raccogliere informazioni e tenere traccia, per ogni Responsabile del trattamento dei dati, della loro certificazione, del codice di condotta approvato e degli impegni pubblicamente vincolanti per il rispetto delle norme applicabili in materia di protezione dei dati.	Nel caso in cui il Responsabile del trattamento non sia certificato e non sia vincolato da un codice di condotta riconosciuto, dovrebbe almeno impegnarsi pubblicamente a rispettare gli obblighi e i principi di protezione dei dati contenuti nel GDPR attraverso uno strumento contrattualmente vincolante (e.g. privacypact o equivalente). Le tre opzioni possono essere cumulate per aumentare il livello di fiducia. Ove applicabile, il Richiedente deve tenere un registro dei propri Responsabili del trattamento dei dati con il loro stato di certificazione, il loro codice di condotta, le norme vincolanti d'impresa e i loro impegni pubblici contrattualmente vincolanti a rispettare il GDPR.	Comunicazione con i Responsabili del trattamento. Registro dei Responsabili del trattamento con certificazioni, codici di condotta o strumenti di impegno vincolanti.	24.3, 28.5, 25.3, 32.2

G.5.2				**Trattamento sotto l'autorità del Titolare o del Responsabile del trattamento**				**29**
G.5.2.1	P	S	A	Trattamento solo su istruzione	SE il Richiedente agisce come Responsabile del trattamento, ALLORA: A) Il Richiedente deve avere regole, una procedura o un meccanismo per: a.1) impedire il trattamento dei dati senza istruzioni del Titolare del trattamento; a.2) (E) ricevere e registrare le istruzioni del Titolare del trattamento. E B) Il Richiedente deve avere un registro delle: b.1) istruzioni di trattamento ricevute dal Titolare; b.2) (E) attività di trattamento. E C) Le attività di trattamento dovranno essere conformi alle istruzioni ricevute dal Titolare.	In qualità di Responsabile del trattamento, il Richiedente deve dimostrare che tratterà i dati soltanto in base e in conformità alle istruzioni ricevute dal Titolare del trattamento.	Regole, procedure o meccanismi in atto per effettuare trattamenti solo sulla base di istruzioni. Registri delle istruzioni ricevute per il trattamento dei dati.	29
G.5.3				**Registri delle attività di trattamento**				**30**
G.5.3.1	C	G	A	Registro del trattamento dei dati da parte del Titolare del trattamento	SE il Richiedente agisce come Titolare del trattamento ALLORA: A) Il Richiedente manterrà un registro scritto (anche in formato elettronico) delle attività di trattamento, che conterrà le seguenti informazioni: a.1) il nome e i dati di contatto del Titolare del trattamento; a.2) (E) se applicabile, il nome e i dati di contatto dei Contitolari del trattamento; a.3) (E) se applicabile, il nome e i dati di contatto del rappresentante del Titolare del trattamento; a.4) (E) il nome e i dati di contatto del responsabile della protezione dei dati; a.5) (E) le finalità del trattamento; a.6) (E) la descrizione delle categorie di interessati e di dati personali; a.7) (E) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati (compresi i destinatari in paesi terzi o organizzazioni internazionali); a.8) (E) la policy di conservazione dei dati che specifica i termini previsti per la cancellazione delle diverse categorie di dati; a.9) (E) la descrizione generale delle misure di sicurezza tecniche e organizzative. E B) SE i dati personali sono trasferiti a paesi terzi ALLORA: b.1) le informazioni sui trasferimenti di dati personali a un paese terzo o a un'organizzazione internazionale; b.2) (E) l'elenco dei paesi terzi o delle organizzazioni internazionali a cui vengono trasferiti i dati; b.3) (E) la documentazione delle misure di salvaguardia messe in atto per mitigare il rischio di tale trasferimento (vedere G.10.5.2).	L'esistenza di un registro delle attività di trattamento è necessaria per la certificazione Europrivacy. Il registro deve essere in formato scritto, anche elettronico, come ad esempio una banca dati. La descrizione delle misure tecniche e organizzative deve tenere conto dell'ambito di applicazione dell'art. 32 del GDPR.	Registro delle attività di trattamento	30

G.5.3.2	P	G	A	Registro delle attività di trattamento in qualità di Responsabile del trattamento	SE il Richiedente agisce come Responsabile del trattamento, ALLORA: A) Il Richiedente deve tenere un registro di tutte le categorie di attività di trattamento svolte nel Target of Evaluation per conto del Titolare, con le seguenti informazioni: a.1) il nome e i dati di contatto del Titolare del trattamento; a.2) (E) se applicabile, il nome e i dati di contatto dei contitolari; a.3) (E) se applicabile, il nome e i dati di contatto del rappresentante del Titolare del trattamento; a.4) (E) il nome e i dati di contatto del responsabile della protezione dei dati; a.5) (E) la descrizione generale delle misure di sicurezza tecniche e organizzative adottate. E B) SE i dati personali sono trasferiti a paesi terzi ALLORA: b.1) le informazioni sui trasferimenti di dati personali a un paese terzo o a un'organizzazione internazionale; b.2) (E) l'elenco dei paesi terzi o delle organizzazioni internazionali a cui vengono trasferiti i dati. b.3) (E) la documentazione delle misure di salvaguardia messe in atto per mitigare il rischio di tale trasferimento (vedere G.10.5.2).	L'esistenza di un registro delle attività di trattamento è necessaria per la certificazione Europrivacy. Il registro deve essere in formato scritto, anche elettronico, come ad esempio una banca dati. La descrizione delle misure tecniche e organizzative deve tenere conto dell'ambito di applicazione dell'art. 32 del GDPR.	Registro delle attività di trattamento	30.2
G.5.3.3	CP	S	A	Registro delle istruzioni per il trattamento dei dati	A) Esiste un registro e/o una documentazione delle istruzioni comunicate dal Titolare del trattamento ai Responsabili del trattamento (o, se del caso, dal Responsabile del trattamento ai Sub-Responsabili).	Il Richiedente deve essere in grado di dimostrare che i dati sono stati trattati dai responsabili del trattamento solo secondo le istruzioni.	Ispezione. Registri di istruzioni per il trattamento dei dati. Colloquio con il CISO o il DPO.	
G.5.3.4	CP	S	A	Completezza del registro	A) Tutte le attività di trattamento nell'ambito del Target of Evaluation devono essere inserite nel Registro delle attività di trattamento.	Il registro delle attività di trattamento deve essere completo ed esaustivo rispetto a tutte le attività di trattamento dei dati. Il Richiedente deve garantire che il registro sia aggiornato frequentemente, ad esempio attraverso una procedura o un meccanismo formale.	Intervista del DPO. Registro delle attività di trattamento.	

G.6				Sicurezza del trattamento e Data Protection by Design Obiettivo: Garantire che i dati trattati nell'ambito del Target of Evaluation beneficino di un'adeguata sicurezza e di una protezione dei dati di tipo "by design" e "by default".				
G.6.1				**Protezione dei dati by design e by default**				**25**
G.6.1.1	C	S	A	Protezione dei dati per progettazione e per impostazione predefinita	A) Il Richiedente deve disporre di policy, regole o procedure che richiedano di applicare e mantenere la protezione dei dati by design e by default per il suo trattamento dei dati, compresa la minimizzazione: a.1) della raccolta e del trattamento dei dati personali; a.2) (E) dell'archiviazione e della conservazione dei dati personali; a.3) (E) dell'accesso ai dati personali trattati. E B) Il Richiedente deve aver valutato formalmente il trattamento dei dati del Target of Evaluation per soddisfare il requisito della protezione dei dati by design e by default, anche attraverso: b.1) una analisi dei rischi per la libertà e i diritti degli interessati in termini di probabilità e gravità; b.2) (E) una valutazione per comprendere se la raccolta dei dati personali è stata limitata all'adempimento delle sue finalità e della sua base giuridica e, in caso contrario, formulare raccomandazioni; b.3) (E) una valutazione per comprendere se il trattamento dei dati personali è limitato all'adempimento della sua finalità e base giuridica e, in caso contrario, formulare raccomandazioni; b.4) (E) una valutazione per comprendere se il periodo di conservazione dei dati personali è limitato all'adempimento della sua finalità e della sua base giuridica e, in caso contrario, formulare raccomandazioni; b.5) (E) una valutazione per comprendere se l'accesso ai dati personali trattati è limitato a chi ha bisogno di accedervi per i propri trattamenti e, in caso contrario, di formulare raccomandazioni; b.6) (E) una valutazione in merito a dove si debbano applicare la crittografia, la pseudonimizzazione e le tecniche di anonimizzazione. E C) il DPO o un esperto con competenze adeguate deve confermare che: c.1) l'analisi e le raccomandazioni sono adeguate; c.2) (E) non ha individuato soluzioni meno invasive per la privacy in termini di raccolta di dati personali per ottenere gli stessi risultati e fornire gli stessi servizi; c.3) (E) le raccomandazioni applicabili sono state implementate.	Il principio della privacy by design stabilisce che qualsiasi azione che comporti il trattamento di dati personali deve essere eseguita tenendo conto della protezione di tali dati, in ogni fase del loro ciclo di vita, implementando tutte le misure necessarie in materia di privacy fin dalla loro progettazione. Il principio della privacy by default stabilisce che il Titolare del trattamento deve implementare misure di sicurezza tecniche e organizzative adeguate per garantire che solo i dati personali necessari per ogni specifica finalità del trattamento siano trattati durante tutto il loro ciclo di vita. Il Richiedente deve tenere un registro di: - analisi del trattamento dei dati da certificare dal punto di vista della protezione dei dati by design; - misure tecniche e organizzative efficaci che sono state implementate per proteggere il trattamento dei dati; - se del caso, le ragioni della mancata attuazione delle misure individuate. Le misure di minimizzazione dei dati devono tenere conto dei requisiti specifici relativi al trattamento dei dati a fini di archiviazione, ricerca o statistica (ad es. art. 89 del GDPR).	Policy, regole e procedure. Interviste dei dipendenti, del CISO e del DPO. Ispezione. Valutazione e dichiarazione del DPO.	25.1
G.6.1.2	C	S	A	Minimizzazione dei dati per impostazione predefinita	A) Il Richiedente deve aver implementato misure tecniche per: a.1) limitare l'accesso ai dati personali sulla base di un registro del personale autorizzato; a.2) (E) è stata utilizzata l'analisi dei rischi per implementare le misure tecniche e organizzative atte a mitigare i rischi identificati; a.3) (E) cancellare o rendere anonimi i dati personali al termine del periodo di conservazione.	La minimizzazione dei dati stabilisce che la quantità di dati personali trattati deve essere limitata al minimo necessario. La conservazione di dati personali non necessari rappresenta di per sé un rischio potenziale per la privacy degli interessati. Il Richiedente deve tenere una documentazione che dimostri che, per impostazione predefinita, tutti i dati personali raccolti sono: - adeguati (sufficienti per un adeguato rispetto delle finalità dell'attività di trattamento); - pertinenti (in relazione alle finalità del trattamento); - limitati (non conservare i dati personali quando non sono necessari). GDPR Art. 11 dovrebbe essere preso in considerazione.	Regole, policy e procedure interne. Interviste dei dipendenti, del CISO e del DPO. Ispezione.	25.2

G.6.2				Sicurezza del trattamento				32
G.6.2.1	CP	G	A	Policy di sicurezza	A) Il Richiedente deve disporre di regole e/o policy di sicurezza scritte per proteggere e mettere in sicurezza il trattamento dei dati, che coprono almeno: a.1) la policy di riservatezza dei dati; a.2) (E) la policy di minimizzazione dei dati; a.3) (E) la policy di accesso ai dati; a.4) (E) le restrizioni al trattamento dei dati (su istruzione); a.5) (E) la policy di archiviazione e conservazione dei dati; a.6) (E) la policy di continuità dei dati e di backup; a.7) (E) la policy sulla violazione dei dati; a.8) (E) le restrizioni sulla copia dei dati e sul "bringing your own device".	Il Richiedente deve disporre di una procedura per: - analizzare e identificare i rischi legati alla sicurezza del trattamento e alle libertà e ai diritti degli interessati; - analizzare la fattibilità, i costi e i benefici delle misure individuate; - documentare e registrare l'analisi del rischio di sicurezza; - garantire che l'analisi del rischio di sicurezza (informatica) e i test siano rinnovati almeno una volta all'anno. Il Richiedente deve tenere un registro: - delle policy e linee guida di sicurezza; - degli audit e/o delle certificazioni di sicurezza; - delle valutazioni del rischio di sicurezza; - dell'efficacia delle misure tecniche e organizzative che sono state implementate per proteggere il trattamento dei dati; - se del caso, delle ragioni della mancata attuazione delle misure individuate. Le misure tecniche e organizzative devono tenere in considerazione: - lo stato dell'arte; - i costi di implementazione; - la natura del trattamento; - l'ambito del trattamento; - il contesto del trattamento; - le finalità del trattamento; - il rischio per i diritti e le libertà delle persone fisiche; - la probabilità e la gravità del rischio. Il riesame del livello di sicurezza dei dati personali trattati deve avvenire secondo un calendario prestabilito (si raccomanda di eseguirlo almeno una volta all'anno) e in caso di modifiche al contesto delle attività di trattamento dei dati. La policy di sicurezza deve anche tenere conto delle normative nazionali complementari applicabili.	Regole e policy di sicurezza. Intervista dei dipendenti, del CISO e del DPO.	32.1
G.6.2.2	CP	G	A	Trattamento solo su istruzione	A) Il Richiedente deve disporre di regole, policy, clausole contrattuali, linee guida o meccanismi per garantire che qualsiasi persona fisica che agisce sotto la sua autorità non tratti i dati personali se non su istruzione del Titolare del trattamento (a meno che non sia obbligata a farlo per legge).	Il Richiedente deve tenere un registro con: - le persone fisiche autorizzate al trattamento dei dati personali; - le attività di trattamento dei dati; - le istruzioni comunicate alla persona fisica sotto la sua autorità per il trattamento dei dati personali con la/e data/e.	Regole e policy di sicurezza. Intervista dei dipendenti, del CISO e del DPO.	32.4
G.6.2.3	CP	G	A	Obbligo contrattuale di riservatezza	A) Il Richiedente deve disporre di regole, policy o procedure per garantire che tutte le persone fisiche che entrano in contatto con i dati personali siano tenute alla riservatezza. obblighi che si estendono oltre la fine delle loro attività.	Il Richiedente deve assicurarsi che tutti coloro che possono accedere ai dati personali siano contrattualmente vincolati a mantenere la riservatezza su tutte le informazioni relative ai dati personali, anche dopo la fine del loro rapporto di lavoro con il Richiedente.	Regole, policy e procedure. Analisi del campione. Intervista del DHR, del DPO e dei dipendenti.	32

G.6.2.4	CP	S	A	Valutazione dei rischi per il trattamento dei dati	A) Il Richiedente deve aver valutato con una metodologia ripetibile i rischi sui trattamenti che possono avere un impatto sui diritti e sulle libertà delle persone fisiche, prendendo in considerazione almeno i rischi di: a.1) distruzione o perdita accidentale o illecita dei dati personali; a.2) (E) alterazione accidentale o illecita dei dati personali; a.3) (E) divulgazione e accesso accidentali, illegali o non autorizzati ai dati personali; a.4) (E) attacchi di intrusione; a.5) (E) il rischio legato all'accesso ai profili ad alto privilegio. E B) I rischi identificati nell'analisi dei rischi devono essere integrati da raccomandazioni e/o da un piano di riduzione del rischio per mitigare i rischi identificati. E C) Ove applicabile, la valutazione dei rischi deve essere aggiornata tenendo conto delle raccomandazioni e/o del piano di mitigazione del rischio. E D) Se la valutazione del rischio conclude che un piano d'azione è una condizione per mitigare il rischio ad un livello accettabile, allora le misure di mitigazione fornite dalla valutazione del rischio devono essere implementate.	La valutazione dei rischi di cui al punto G.6.2.4 è sempre necessaria ed è parte della valutazione richiesta al punto G8.2.2 quando è richiesta una Valutazione d'Impatto sulla Protezione dei Dati (DPIA) (vedi criterio G.8.1.1). Il Richiedente deve anche valutare i rischi relativi alla sicurezza e alla disponibilità del trattamento dei dati. Il Richiedente deve definire la metodologia di valutazione dei rischi da seguire. La metodologia deve considerare sia la probabilità che l'impatto potenziale di ogni rischio identificato. Metodologie standard come la ISO 31000 possono essere considerate adeguate. La valutazione del rischio deve tenere conto anche della natura dei dati trattati e se il trattamento dei dati personali può comportare un rischio elevato per i diritti e le libertà delle persone fisiche. Ciò avviene quando il Richiedente utilizza nuove soluzioni tecnologiche o organizzative, raccoglie dati relativi a interessati vulnerabili, tratta dati su larga scala, dati sensibili o dati altamente personali, o utilizza strumenti per il monitoraggio sistematico. Il Richiedente deve quindi considerare e valutare almeno i rischi di: - distruzione o perdita accidentale o illegale dei dati personali; - alterazione accidentale o illecita dei dati personali; - divulgazione e accesso accidentale, illegale o non autorizzato dei dati personali e l'inversione non autorizzata della pseudonimizzazione; Il rischio di rivelare dati sensibili, altamente personali, dati di persone vulnerabili, dati biometrici o altri dati che possono dare origine a discriminazioni o a un significativo svantaggio socioeconomico deve essere considerato di impatto elevato. Il Richiedente deve tenere una chiara traccia delle valutazioni del rischio effettuate, dei rischi identificati come risultato di tali valutazioni e delle azioni di mitigazione e/o contingenza intraprese o adottate in risposta a tali valutazioni. È importante ricordare che ogni criterio applicabile deve essere soddisfatto singolarmente e le misure identificate dalla valutazione del rischio devono essere affrontate. Nel caso in cui le raccomandazioni della valutazione del rischio vadano oltre i requisiti di altri criteri, i primi devono comunque essere soddisfatti.	Revisione della documentazione del report di analisi dei rischi. Valutazione dei metodi utilizzati per valutare il rischio.	32.2
G.6.2.5	CP	S	A	Policy e registro dei diritti di accesso	A) Il Richiedente deve aver stabilito una policy di controllo degli accessi che si articola attorno a ruoli e responsabilità. E B) Il Richiedente deve tenere un registro aggiornato dei diritti di accesso dei suoi dipendenti e dei suoi collaboratori che possono accedere ai dati personali. E C) Il Richiedente deve avere una procedura, una policy o un meccanismo in atto per rivedere regolarmente il registro dei diritti di accesso. E D) La policy dei diritti di accesso deve essere applicata e verificabile per entrambi: d.1) l'accesso fisico al luogo in cui sono conservati i dati; d.2) l'accesso elettronico agli insiemi di dati personali.	Il Richiedente deve disporre di una policy di controllo degli accessi completa, definita in base a ruoli e responsabilità. Tale policy deve essere integrata da un registro dei diritti di accesso e deve essere conforme al principio del minor privilegio. Il corrispondente La policy/il registro devono fornire un'adeguata giustificazione dei diritti di accesso concessi a ciascuna categoria di dipendenti o a ciascun dipendente.	Registro dei diritti di accesso. Ispezione.	32
G.6.2.6	CP	S	A	Log di accesso e trasferimento	A) Il Richiedente deve avere un sistema di monitoraggio, un meccanismo o un processo in atto per registrare e tenere un registro: a.1) dell'accesso ai dati personali da parte di dipendenti e agenti del Richiedente; a.2) (E) del trasferimento di dati personali a terzi, compresi i responsabili del trattamento ed i trasferimenti transfrontalieri.	La Policy deve essere specifica e dettagliata. Il sistema di monitoraggio deve essere affidabile e sufficientemente robusto rispetto allo stato dell'arte della tecnologia per proteggere i diritti e le libertà degli interessati.	Ispezione. Log di accesso e di trasferimento. Intervista del CISO o del DPO.	32

G.6.2.7	CP	S	A	Continuità, integrità e disponibilità	A) Il Richiedente deve disporre di policy, procedure o piani per garantire la continuità del trattamento e dei servizi associati in caso di incidenti fisici o tecnici, tra cui: a.1) per garantire la costante riservatezza e integrità dei dati personali; a.2) (E) per garantire la disponibilità e la resilienza dell'accesso degli interessati ai loro dati personali.	Il Richiedente deve elaborare un piano di continuità per ripristinare la disponibilità dei dati in caso di incidenti tecnici o fisici, come cyberattacchi, ransomware, crash hardware.	Regole e policy di sicurezza. Piano di continuità. Intervista dei dipendenti, del CISO e del DPO.	32.1.b
G.6.2.8	CP	S	A	Crittografia delle comunicazioni	A) Quando le comunicazioni di dati personali attraverso le reti pubbliche possono essere criptate, esse devono essere criptate.	Ove applicabile, il Richiedente deve criptare il trasferimento elettronico e la comunicazione dei dati personali al di fuori dei propri locali, anche utilizzando https per i dati personali raccolti o visualizzati su interfacce web. Dovrebbe tenere conto delle normative applicabili in materia di crittografia e della fattibilità tecnica di tale crittografia.	Ispezione. Analisi a campione.	32.1.a
G.6.2.9	CP	S	A	Obbligo di backup	A) I dati personali memorizzati dal Richiedente devono essere sottoposti a backup.	Il Richiedente deve eseguire il backup e testare regolarmente la sua capacità di ripristinare i set di dati dai suoi backup. Un criterio complementare è incluso nelle verifiche e nei controlli tecnici e organizzativi (T.1.3.1) per valutare la capacità del Richiedente di ripristinare i dati con i propri file di backup.	Ispezione. Analisi a campione. Report del test di backup-ripristino.	32.1.c
G.6.2.10	CP	S	A	Requisiti contestuali complementari	A) Le attività di trattamento dei dati del Target of Evaluation saranno conformi alle Verifiche e Controlli Contestuali Complementari applicabili specificati da Europrivacy.	Europrivacy mantiene un elenco completo di verifiche e controlli contestuali complementari applicabili a specifiche attività di trattamento dei dati. L'elenco dei requisiti deve essere utilizzato dal Richiedente per preparare la propria certificazione e può essere comunicato agli auditor.	Report delle Verifiche e dei Controlli Contestuali. Audit complementari. Ispezione. Valutazione e dichiarazione del DPO.	5, 24, 25, 32, 35
G.6.2.11	CP	S	A	Misure tecniche e organizzative complementari	A) Il Richiedente deve: a.1) aver valutato l'adeguatezza delle sue Misure Tecniche e Organizzative (TOM); a.2) (OPPURE) avere una certificazione complementare delle misure tecniche e organizzative adottate per garantire la sicurezza e la protezione dei dati trattati nell'ambito del Target of Evaluation. E B) La valutazione delle TOM deve essere stata convalidata dal DPO come sufficiente e adeguata a proteggere i diritti e le libertà degli interessati.	Europrivacy mantiene un elenco completo di verifiche e controlli delle Misure Tecniche e Organizzative. L'elenco è messo a disposizione del Richiedente e può essere compilato e comunicato agli auditor. In caso di dubbi sulla valutazione e sulle conclusioni del DPO, l'Auditor deve contestare la conclusione e richiedere una valutazione complementare.	Ispezione. Report di valutazione delle Misure Tecniche e Organizzative. Audit complementare. Ispezione. Valutazione e dichiarazione del DPO.	32

G.7				Gestione delle violazioni dei dati Obiettivo: Garantire che le violazioni dei dati relativi al Target of Evaluation siano gestite in conformità ai requisiti normativi.				
G.7.1				**Notifica di una violazione dei dati personali all'Autorità di Controllo**				**33**
G.7.1.1	CP	G	A	Obbligo di documentare le violazioni dei dati	A) Il Richiedente deve tenere un registro delle proprie violazioni dei dati che comprenda almeno: a.1) i fatti relativi alla violazione dei dati personali; a.2) (E) gli effetti della violazione dei dati; a.3) (E) l'azione correttiva intrapresa.	Il Richiedente deve disporre del registro anche se non si è ancora verificata alcuna violazione.	Registro delle violazioni dei dati.	33,5
G.7.1.2	C	G	A	Obbligo di notifica e comunicazione delle violazioni dei dati da parte del Titolare del trattamento	A) Il Richiedente deve avere regole, una procedura o un meccanismo per: a.1) registrare le violazioni dei dati e le azioni di follow-up con data e ora; a.2) (E) valutare se la violazione dei dati può comportare un rischio per i diritti e le libertà delle persone fisiche; a.3) (E) determinare e intraprendere azioni appropriate per ridurre al minimo i rischi e la loro probabilità, e l'impatto potenziale sui soggetti interessati; a.4) (E) se il rischio può comportare un rischio per i diritti e le libertà delle persone fisiche, informare l'Autorità di Controllo senza indebito ritardo e non oltre 72 ore dopo esserne venuti a conoscenza; a.5) (E) se il rischio può comportare un rischio per i diritti e le libertà delle persone fisiche, informare l'interessato senza indebito ritardo (salvo che non sia richiesto dalla normativa).	Il Richiedente deve tenere un registro di: - tutte le violazioni di dati identificate con data e ora; - i fatti relativi alla violazione dei dati; - gli effetti della violazione dei dati; - le comunicazioni relative alle violazioni dei dati; - le azioni di follow-up e di rimedio intraprese con la data e l'ora; - se del caso, i motivi della mancata comunicazione all'Autorità di Controllo. Tutte le violazioni registrate (se esistenti) che hanno esposto a rischio i diritti e la libertà degli interessati negli ultimi 12 mesi devono essere comunicate all'Autorità di Controllo entro il limite di 72 ore. Nel parere 03/2014 sulla notifica delle violazioni, il WP29 ha spiegato che le violazioni possono essere classificate in base ai tre noti principi di sicurezza delle informazioni: - "Violazione della riservatezza": quando si verifica una divulgazione o un accesso non autorizzato o accidentale ai dati personali. - "Violazione dell'integrità": quando si verifica un'alterazione non autorizzata o accidentale dei dati personali. - "Violazione della disponibilità": quando si verifica una perdita accidentale o non autorizzata dell'accesso ai dati personali o la loro distruzione. Per quanto riguarda le eccezioni di cui al requisito a.5), l'art. 34.2 del GDPR specifica le eccezioni applicabili ai sensi del GDPR.	Regole, procedure o meccanismi. Registro delle violazioni dei dati. Intervista dei dipendenti e del DPO. Ispezione. Test della procedura.	33.1, 34.1
G.7.1.3	P	G	A	Obbligo del Responsabile del trattamento di comunicare le violazioni dei dati senza indebito ritardo	A) Il Richiedente deve avere regole, una procedura o un meccanismo per: a.1) registrare le violazioni dei dati e le azioni di follow-up con data e ora; a.2) (E) determinare e intraprendere le azioni appropriate per ridurre al minimo i rischi e il potenziale impatto sulle persone interessate. a.3) (E) assistere il Titolare del trattamento nella valutazione del rischio della violazione dei dati per i diritti e le libertà delle persone fisiche; a.4) (E) comunicare la violazione al/i relativo/i Titolare/i del trattamento dei dati senza indebito ritardo.	I Responsabili del trattamento (e i Sub-Responsabili del trattamento) devono disporre di regole, procedure o meccanismi adeguati per garantire che qualsiasi violazione venga affrontata e comunicata ai relativi titolari del trattamento senza indebito ritardo. Occorre tenere presente che i Titolari del trattamento devono rispettare scadenze molto rigide per affrontare, notificare e comunicare la violazione, a seconda dei casi. I responsabili del trattamento non devono ritardare tali comunicazioni.	Policy, regole e procedure. Interviste dei dipendenti, del CISO e del DPO. Ispezione.	33.2
G.7.1.4	C	G	A	Requisiti di notifica	A) La procedura per la notifica di una violazione dei dati all'Autorità di Controllo richiede al suo interno le seguenti informazioni: a.1) la natura della violazione dei dati personali; a.2) (E) le categorie e il numero approssimativo di interessati e di dati personali coinvolti (ove possibile); a.3) (E) il nome e i dati di contatto del responsabile della protezione dei dati o di un altro punto di contatto per ottenere ulteriori informazioni; a.4) (E) le probabili conseguenze della violazione dei dati personali; a.5) (E) le misure adottate o che si propone di adottare il Titolare del trattamento per far fronte alla violazione dei dati personali, comprese, se del caso, le misure volte ad attenuarne i possibili effetti negativi.	Il Richiedente deve disporre di un modello per le notifiche. La procedura di notifica deve contenere le seguenti informazioni: - la natura della violazione dei dati personali; - le categorie e il numero approssimativo di interessati e di dati personali coinvolti (ove possibile); - il nome e i dati di contatto del responsabile della protezione dei dati o di un altro punto di contatto per ottenere ulteriori informazioni; - le probabili conseguenze della violazione dei dati personali; - le misure adottate o proposte dal Titolare del trattamento per far fronte alla violazione dei dati personali, comprese, se del caso, le misure per attenuarne i possibili effetti negativi.	Regole, procedure o meccanismi. Registro delle violazioni di dati. Intervista dei dipendenti e del DPO. Ispezione. Test della procedura.	33.3

G.7.2				Comunicazione di una violazione dei dati personali all'interessato				34
G.7.2.1	C	G	A	Requisiti per la comunicazione delle violazioni	A) La procedura o il meccanismo di comunicazione di una violazione dei dati agli interessati deve comprendere almeno le seguenti informazioni: a.1) la natura della violazione dei dati personali; a.2) (E) le categorie di dati personali interessate; a.3) (E) il nome e i dati di contatto del responsabile della protezione dei dati o di un altro punto di contatto per ottenere ulteriori informazioni; a.4) (E) le probabili conseguenze della violazione dei dati personali; a.5) (E) le misure adottate o proposte dal Titolare del trattamento (e/o raccomandate agli interessati) per affrontare la violazione dei dati personali, comprese, se del caso, le misure per attenuarne i possibili effetti negativi.	Il Richiedente deve tenere registri documentati di: - tutte le violazioni di dati identificate con data e ora; - i fatti relativi alla violazione dei dati; - gli effetti della violazione dei dati; - le comunicazioni relative alle violazioni dei dati; - le azioni di follow-up e di rimedio intraprese con la data e l'ora; - se del caso, i motivi per cui non sono stati informati gli interessati. La dimostrazione può essere effettuata tramite un campionamento di registri passati, un esercizio documentato o una dimostrazione tecnica. Esempi di pregiudizio per gli interessati sono: discriminazione, furto d'identità o frode, perdite finanziarie e danni alla reputazione; quando la violazione comprende dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, la religione o le convinzioni filosofiche, o l'appartenenza sindacale, o che includano dati genetici, dati relativi alla salute o alla vita sessuale, o condanne penali e reati o relative misure di sicurezza.	Registri delle violazioni e delle comunicazioni. Policy, regole e procedure. Intervista dei dipendenti e del DPO.	34.2
G.7.2.2	C	S	E	Esenzioni tollerate	SE sono soddisfatte le seguenti condizioni, ALLORA la comunicazione diretta all'interessato non è richiesta: A) La comunicazione non è stata effettuata a causa di una delle seguenti eccezioni: a.1) il Richiedente ha implementato misure tecniche e organizzative adeguate (come la crittografia) per rendere i dati personali violati incomprensibili a chiunque non sia autorizzato ad accedervi. a.2) (OPPURE) il Titolare del trattamento ha adottato misure successive che garantiscono che il rischio elevato per i diritti e le libertà degli interessati non è più probabile che si verifichi; a.3) (OPPURE) l'informazione diretta avrebbe richiesto uno sforzo sproporzionato ED è stata sostituita da una comunicazione pubblica (o da una misura analoga che consenta di informare gli interessati in modo altrettanto efficace). E B) La violazione dei dati non può comportare un rischio elevato per i diritti e le libertà degli interessati.	Qualsiasi esenzione deve essere chiaramente giustificata e documentata. Anche se il GDPR autorizza alcune esenzioni, Europrivacy incoraggia i Richiedenti ad adottare una politica conservativa a favore dei diritti e delle libertà degli interessati, riducendo al minimo il ricorso alle esenzioni.	DPO, registri, policy e procedure interne, test e verifiche, ispezioni, colloqui.	34.3

G.8				Valutazione d'impatto sulla protezione dei dati (DPIA) Obiettivo: Garantire che, se il trattamento dei dati nell'ambito del Target of Evaluation richiede una valutazione d'impatto sulla protezione dei dati, quest'ultima sia effettuata in conformità con i requisiti normativi.				
G.8.1				**Obbligo di valutare se è necessaria una valutazione d'impatto sulla protezione dei dati (DPIA)**				**35**
G.8.1.1	C	S	A	Valutazione d'impatto sulla protezione dei dati (DPIA)	A) Il Richiedente deve aver eseguito una DPIA se uno dei seguenti casi si applica al Target of Evaluation: a.1) il trattamento dei dati comporta un rischio intrinseco elevato per i diritti e le libertà dell'interessato; a.2) (OPPURE) una valutazione sistematica degli aspetti personali delle persone fisiche basata su un trattamento automatizzato (come la profilazione) che può riguardare le persone fisiche; a.3) (OPPURE) un trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali o reati; a.4) (OPPURE) il trattamento rientra nell'elenco delle attività di trattamento dei dati che richiedono una DPIA pubblicato dall'Autorità di Controllo del Richiedente; a.5) (OPPURE) operazioni di trattamento elencate come richiedenti la DPIA secondo la Autorità di Controllo o la legislazione applicabile. E B) Il Richiedente deve aver eseguito una DPIA, tranne nel caso in cui il DPO: b.1) ha effettuato una valutazione preliminare scritta dei rischi per i diritti e le libertà degli interessati; b.2) (E) ha concluso, nella sua valutazione scritta, che non esiste un rischio elevato per il diritti e libertà degli interessati; b.3) (E) è in atto una procedura, una policy o un piano per rivalutare il rischio su base regolare. E C) Il Richiedente deve disporre di policy, regole o procedure per la revisione delle proprie conclusioni di non effettuare una DPIA quando l'ambito o la finalità del trattamento del Target of Evaluation sono sostanzialmente modificati o esposti a nuovi rischi.	Una DPIA può riguardare un singolo trattamento di dati o più trattamenti simili per natura, ambito, contesto, finalità e rischi. Può anche essere utile per valutare l'impatto sulla protezione dei dati di un prodotto tecnologico. La DPIA deve prendere in considerazione tutti i rischi per i diritti e le libertà degli interessati. I criteri forniti dalle linee guida del WP29 (WP248 rev.01) (pagg. 9-11) devono essere presi in considerazione per identificare un rischio elevato per l'interessato. Il Richiedente deve effettuare una DPIA per qualsiasi trattamento dei dati che coinvolga: - valutazione o scoring - decisioni automatizzate con effetti giuridici o analoghi significativi - monitoraggio sistematico - dati sensibili o di natura altamente personale - trattamento dei dati su larga scala - abbinare o combinare insiemi di dati - dati relativi a interessati vulnerabili - uso o applicazione innovativa di nuove soluzioni tecnologiche o organizzative - trattamenti che impediscono agli interessati di esercitare un diritto o di usufruire di un servizio o di un contratto. Il Richiedente deve tenere registri documentali con: - la valutazione dell'applicabilità e della rilevanza della DPIA; - se applicabile, la documentazione e le conclusioni della DPIA; - se applicabile, le azioni di follow-up e di rimedio intraprese con la data e l'ora; - se applicabile, le ragioni per cui non è stata effettuata la DPIA o per cui non sono state attuate le raccomandazioni di una DPIA effettuata.	Report e documentazione della DPIA. Valutazione preliminare da parte del DPO. Dichiarazione del DPO. Intervista del DPO.	35.1, 35.3, 35.4
G.8.1.2	C	S	E	Esenzione tollerata	La DPIA non è necessaria (tranne se richiesta dallo Stato membro) se: A) Il trattamento ha una base giuridica nel diritto dell'Unione o degli Stati membri e il Titolare del trattamento è soggetto a a tale legge E una valutazione d'impatto è già stata effettuata su trattamenti di dati simili che: b.1) coinvolgono interessati simili; b.2) (E) per scopi analoghi. O B) Il Target of Evaluation rientra nell'elenco delle attività di trattamento dei dati esentate dalla DPIA dall'autorità nazionale di vigilanza.	Qualsiasi esenzione deve essere chiaramente giustificata e documentata. Ad esempio, il Target of Evaluation potrebbe rientrare nell'elenco nazionale dei trattamenti esclusi dall'obbligo di DPIA, ai sensi dell'art. 35(5) del GDPR.	Legge pertinente	35.10.

G.8.2				Requisiti della valutazione d'impatto sulla protezione dei dati (DPIA) Condizione:	SE è applicabile una DPIA ALLORA:			27
G.8.2.1	C	S	A	Requisiti del processo DPIA	A) Il processo di DPIA deve avere: a.1) coinvolto il DPO nella progettazione e nel monitoraggio del processo di DPIA; a.2) (E) se applicabile, avere coinvolto gli interessati o i loro rappresentanti nella valutazione d'impatto; a.3) (E) se del caso, avere tenuto conto dell'adozione di un codice di condotta, certificazioni e altri impegni vincolanti ed esecutivi, tramite contratti o altri strumenti giuridicamente vincolanti; a.4) (E) se applicabile, ha adottato un piano di azioni correttive; a.5) (E) se del caso, ha intrapreso azioni per affrontare e ridurre i rischi identificati dalla DPIA a un livello valutato dal DPO come accettabile per gli interessati; a.6) (E) ha consultato l'Autorità di Controllo se la DPIA ha concluso che il trattamento comporta rischi elevati per gli interessati.	Il Richiedente deve assicurarsi che il processo di DPIA sia generalmente allineato con il processo iterativo generico per l'esecuzione di una DPIA (linea guida WP29 WP248 rev.1), comprese le seguenti fasi: - descrizione del trattamento previsto - valutazione della necessità e della proporzionalità - specifiche delle misure previste - valutazione dei rischi per i diritti e le libertà degli interessati - definizione delle misure previste per affrontare i rischi - documentazione - monitoraggio e revisione Il parere del DPO deve essere richiesto e documentato insieme alle decisioni prese dal Titolare del trattamento sulla base del parere. L'esecuzione della DPIA deve essere monitorata dal DPO. Il Richiedente può chiedere il parere degli interessati o dei loro rappresentanti con vari mezzi a seconda del contesto (sondaggi, questionari, ecc.) e, se la decisione finale si discosta dal parere degli interessati, la ragione deve essere documentata. Deve essere preparata anche la documentazione relativa alla ragione per cui non è stato richiesto il parere degli interessati.	Report e documentazione della DPIA. Intervista del DPO.	35.2, 35.7.b
G.8.2.2	C	S	A	Requisiti di contenuto della DPIA	A) La DPIA deve contenere almeno i seguenti elementi: a.1) la descrizione sistematica delle operazioni di trattamento previste; a.2) (E) le finalità del trattamento dei dati personali; a.3) (E) ove applicabile, il legittimo interesse del Titolare del trattamento; a.4) (E) una valutazione della necessità e della proporzionalità del trattamento rispetto alle finalità; a.5) (E) la valutazione dei rischi per le libertà e i diritti degli interessati; a.6) (E) le misure previste per affrontare i rischi, comprese, se del caso, le salvaguardie, le misure e i meccanismi di sicurezza; a.7) (E) se applicabile, la raccomandazione di consultare l'Autorità di Controllo.	La DPIA deve essere effettuata prima del trattamento e il più presto possibile nella progettazione dell'operazione di trattamento, anche se alcune delle operazioni di trattamento sono ancora sconosciute. La DPIA ai sensi del GDPR è uno strumento per gestire i rischi per i diritti degli interessati. (Linea guida WP29 WP248 rev. 1), il Richiedente deve tenere conto del loro punto di vista quando esegue la valutazione. Quando è previsto un trattamento probabilmente ad alto rischio, il Titolare del trattamento deve (Linea guida WP29 WP248 rev.1 + allegato 2): - scegliere e documentare una metodologia di DPIA appropriata, che descriva sistematicamente il trattamento, ne valuti la necessità e la proporzionalità, gestisca i rischi per i diritti e le libertà degli interessati e coinvolga le parti interessate - integrare la DPIA nei processi di progettazione, sviluppo, cambiamento, rischio e revisione operativa, in conformità con i processi interni, il contesto e la cultura. - coinvolgere le opportune parti interessate e definire chiaramente le loro responsabilità - Fornire la relazione DPIA all'Autorità di Controllo, se richiesto. - Consultare l'Autorità di Controllo se permangono rischi elevati non mitigati. - Rivedere periodicamente la DPIA - Documentare le decisioni prese. Il processo di DPIA prevede che il richiedente abbia una decisione formale basata sulle conclusioni della valutazione e sul parere del DPO, in particolare per quanto riguarda le misure correttive e/o il piano d'azione.	Report e documentazione della DPIA. Intervista del DPO.	35.7

G.8.2.3	C	S	A	Requisito del coinvolgimento degli interessati	A) Il Richiedente deve registrare le opinioni degli interessati e/o dei loro rappresentanti consultati per la valutazione d'impatto (o una giustificazione documentata per il mancato coinvolgimento degli interessati o dei loro rappresentanti).	Il Richiedente può chiedere il parere degli interessati o dei loro rappresentanti con vari mezzi a seconda del contesto (sondaggi, questionari, ecc.) e, se la decisione finale si discosta dal parere degli interessati, la ragione deve essere documentata. Deve essere preparata anche la documentazione relativa alla ragione per cui non è stato richiesto il parere degli interessati. Il Richiedente deve tenere registri documentali con: - la valutazione e la decisione di consultare o meno gli interessati o i loro rappresentanti. - se del caso, le prove della consultazione; - se del caso, le azioni di follow-up e di rimedio intraprese per rispondere alle preoccupazioni degli interessati; - se del caso, i motivi per cui non sono state affrontate le preoccupazioni sollevate dagli interessati. Il Richiedente deve documentare come si è tenuto conto delle preoccupazioni sollevate dagli interessati o dai loro rappresentanti.	Report e documentazione della DPIA. Intervista del DPO.	35.9
G.8.2.4	C	S	A	Revisione della DPIA in caso di modifica dei rischi	A) Il Richiedente deve disporre di regole o procedure per rivedere la DPIA, o la sua decisione di non eseguire una DPIA, ogniqualvolta l'ambito o la finalità del trattamento dei dati del Target of Evaluation siano sostanzialmente modificati o esposti a nuovi rischi.	Il Richiedente deve assicurarsi che la DPIA sia continuamente riesaminata e regolarmente rivalutata e, in particolare, deve effettuare una DPIA ogni qualvolta: - Si è verificata una modifica delle condizioni di attuazione (ambito, finalità, dati personali raccolti, identità dei Titolari o dei destinatari, periodo di conservazione dei dati, misure tecniche e organizzative, ecc.) - si è verificata una modifica del rischio derivante dalle operazioni di trattamento - si è verificata una modifica del contesto organizzativo o sociale dell'attività di trattamento Ove applicabile, il Richiedente deve tenere registri documentali con: - la valutazione e la decisione di rivedere o meno la DPIA. - se applicabile, il riesame della DPIA e le sue conclusioni; - se applicabile, le azioni di follow-up e di rimedio intraprese per rispondere alle risultanze del riesame della DPIA; - se applicabile, le ragioni per cui non si è tenuto conto delle raccomandazioni della DPIA.	Regole e procedure. Intervista del DPO.	35.1.m

G.8.2.5	C	S	A	Obbligo di consultare l'Autorità di Controllo in caso di rischio elevato identificato.	SE una DPIA ha individuato rischi residui elevati per i diritti o la libertà degli interessati, ALLORA: A) Il Titolare del trattamento deve aver: a.1) informato e consultato l'Autorità di Controllo sui rischi individuati; a.2) (E) ricevuto il parere dell'Autorità di Controllo; a.3) (E) se del caso, attuato le azioni raccomandate menzionate nel parere.	Qualora la DPIA riveli rischi residui elevati, il Titolare del trattamento dovrà richiedere la consultazione preventiva dell'Autorità di controllo (articolo 36, (1)). Nell'ambito di tale consultazione, la DPIA deve essere fornita in modo completo (art. 36(3)(e)). Qualora il Titolare del trattamento non riesca a trovare misure sufficienti per ridurre i rischi a un livello accettabile (cioè i rischi residui sono ancora elevati), è necessaria la consultazione dell'Autorità di Controllo. Il Titolare del trattamento dovrà consultare l'Autorità di controllo ogniqualvolta il diritto degli Stati membri preveda che i Titolari del trattamento debbano consultarsi con l'Autorità di Controllo e/o ottenerne l'autorizzazione preventiva in relazione al trattamento da parte di un Titolare del trattamento per l'esecuzione di un compito svolto dal Titolare del trattamento nel pubblico interesse, compreso il trattamento in relazione alla protezione sociale e alla salute pubblica (articolo 36, paragrafo 5). SE l'Autorità di Controllo è stata consultata sulla DPIA, il Richiedente deve fornire le seguenti informazioni all'Autorità di Controllo: - le rispettive responsabilità del Titolare del trattamento, dei Contitolari o dei Responsabili del trattamento; - le finalità e i mezzi del trattamento previsto; - le misure e le garanzie a tutela dei diritti e delle libertà dell'interessato; - i dati di contatto del DPO (ove applicabile); - la valutazione d'impatto sulla protezione dei dati; - qualsiasi altra informazione richiesta dall'Autorità di Controllo. Se è richiesta un'autorizzazione a livello nazionale, l'autorizzazione deve essere stata rilasciata e convalidata nel contesto dei criteri G.1.1.3.	Corrispondenza con l'Autorità di Controllo.	36
G.9				**Responsabile della protezione dei dati (DPO)** Obiettivo: Garantire l'adeguatezza del ruolo, della funzione e della qualifica del responsabile della protezione dei dati incaricato di controllare la conformità del trattamento dei dati nel Target of Evaluation.				
G.9.1				**Designazione del responsabile della protezione dei dati**				**37**
G.9.1.1	CP	G	A	Designazione del responsabile della protezione dei dati	A) Il Richiedente deve aver designato un Responsabile della protezione dei dati.	Mentre il GDPR ammette che la nomina di un DPO non sia sempre necessaria, la certificazione Europrivacy richiede che un DPO sia formalmente nominato. Il DPO può essere esterno o avere altre funzioni, purché non crei un conflitto di interessi. Il DPO deve supervisionare la conformità del trattamento dei dati alla normativa applicabile. Per garantire un'adeguata indipendenza, il DPO non deve essere la persona che determina le finalità del trattamento dei dati.	Intervista del DPO. Contratto del DPO. Sito web del Richiedente.	37.1
G.9.1.2	CP	G	A	Requisiti del DPO	A) Il responsabile della protezione dei dati del Richiedente deve avere un'istruzione in legge o una formazione attestata sulle normative di protezione dei dati.	Il responsabile della protezione dei dati deve avere un'istruzione in legge o una formazione certificata in materia di normative sulla protezione dei dati che dimostri la sua capacità di valutare la conformità delle attività di trattamento dei dati con le normative applicabili in materia di protezione dei dati, compreso il GDPR.	Curriculum del DPO. Intervista del DPO.	37.5
G.9.1.3	CP	G	A	Comunicazione dei dati di contatto del DPO	A) I registri devono dimostrare che i dettagli di contatto e/o il meccanismo per comunicare con il DPO: b.1) sono pubblicati e disponibili per gli interessati; b.2) (E) sono stati comunicati all'Autorità di Controllo.	I dati di contatto del DPO devono essere pubblicati e disponibili per gli interessati e devono essere stati comunicati all'Autorità di controllo. I dati di contatto del DPO non richiedono necessariamente il nome personale del DPO, purché le comunicazioni e le richieste inviate dagli interessati ai dati di contatto indicati siano effettivamente indirizzate al DPO.	Sito web del Richiedente. Corrispondenza con l'Autorità di Controllo.	37.7

G.9.2				Posizione dei responsabili della protezione dei dati				38
G.9.2.1	CP	G	A	Comunicazione del mandato del DPO	A) Il Richiedente deve disporre di regole, policy o procedure che: a.1) richiedono ai dipendenti e alla direzione di informare e coinvolgere tempestivamente il DPO in tutte le questioni relative alla protezione dei dati; a.2) danno autorità e accesso effettivo al DPO per il monitoraggio della conformità delle operazioni di trattamento dei dati personali.	Il Richiedente deve tenere registri documentati delle attività del DPO per dimostrare il suo coinvolgimento nelle questioni relative alla protezione dei dati.	Regole, policy e procedure.	38.1
G.9.2.2	CP	G	A	Supporto al DPO	A) Il Richiedente deve aver stanziato risorse per sostenere la formazione continua e lo sviluppo delle capacità del DPO.	Dovrebbe essere stanziato un budget dedicato alla formazione continua del DPO, come la partecipazione a workshop, webinar, corsi di formazione o conferenze sulla protezione dei dati.	Dotazione di bilancio. Intervista del DPO.	38.2
G.9.2.3	CP	G	A	Indipendenza del DPO	A) Il Richiedente deve aver adottato regole, policy o clausole contrattuali: a.1) tutelare l'autonomia e l'indipendenza decisionale del DPO; a.2) (E) proteggere il DPO da qualsiasi forma di pressione indebita legata allo svolgimento del suo compito; a.3) (E) per consentire al DPO di riferire direttamente al più alto livello dirigenziale del Richiedente.	Il DPO dovrebbe essere completamente indipendente. Ad esempio, l'EDPB non ritiene che la funzione di rappresentante nell'Unione sia compatibile con il ruolo di un responsabile esterno della protezione dei dati ("DPO") che verrebbe istituito nell'Unione. Il rappresentante è infatti soggetto a un mandato da parte di un titolare o di un responsabile del trattamento e agirà per suo conto e quindi sotto le sue dirette istruzioni. Per motivi di imparzialità, il DPO non deve essere stato coinvolto nella definizione e nella gestione delle attività di trattamento dei dati sotto la sua autorità negli ultimi 24 mesi. Il DPO può essere esterno o avere altre funzioni, purché non crei un conflitto di interessi. Il DPO deve supervisionare la conformità del trattamento dei dati alla normativa applicabile. Per garantire un'adeguata indipendenza, il DPO non deve essere la persona che determina le finalità del trattamento dei dati.	Regole, policy e procedure. Contratto del DPO.	38.3
G.9.2.4	CP	G	A	Accesso degli interessati al DPO	A) Gli interessati potranno contattare il DPO dal sito web del Richiedente.	Il Richiedente deve tenere un registro completo con: - le richieste dell'interessato al DPO con la relativa data; - la corrispondenza tra il DPO e gli interessati con la/e data/e; - la valutazione della richiesta e la/e azione/i di follow-up con la/e data/e; - se del caso, le ragioni per cui il DPO non ha dato seguito alla richiesta ricevuta.	Sito web del richiedente. Ispezione. Test della procedura di contatto.	38.4
G.9.2.5	CP	G	A	Clausole contrattuali del DPO	A) Il contratto con il DPO deve contenere clausole: a.1) vincolare il DPO al segreto o alla riservatezza in merito allo svolgimento dei suoi compiti, in conformità al diritto dell'Unione o degli Stati membri; a.2) (E) autorizzare il DPO a collaborare e comunicare con l'Autorità di Controllo; a.3) (E) impegnare il DPO a evitare e segnalare qualsiasi conflitto di interessi.	La clausola di riservatezza dovrebbe far parte degli obblighi contrattuali del DPO. Tuttavia, gli obblighi contrattuali non dovrebbero impedire al DPO di comunicare e condividere informazioni riservate con l'Autorità di Controllo, in conformità al diritto dell'Unione o degli Stati membri. Il Richiedente deve disporre di una procedura per identificare, segnalare e risolvere eventuali conflitti di interesse. Se il DPO svolge altri compiti e mansioni, si raccomanda di disporre di una procedura per valutare il rischio di conflitto di interessi derivante da tali attività complementari. Il Richiedente deve tenere un registro con: - se del caso, qualsiasi rischio di conflitto di interessi individuato; - la valutazione del rischio di conflitto di interessi individuato e le azioni di follow-up; - se il DPO svolge altri compiti e mansioni, la documentazione che dimostra che è stato valutato il rischio di conflitto di interessi con attività complementari. Il DPO può essere esterno o avere altre funzioni, purché non crei un conflitto di interessi. Il DPO deve supervisionare la conformità del trattamento dei dati alla normativa applicabile. Per garantire un'adeguata indipendenza, il DPO non deve essere la persona che determina le finalità del trattamento dei dati.	Contratto del DPO. Regole e policy.	38.5, 38.6

G.9.2.6	CP	G	A	Adeguatezza del tempo di lavoro del DPO	A) Il Richiedente deve aver valutato: a.1) il tempo di lavoro richiesto per il DPO in considerazione le tipologie di trattamento dei dati e i rischi per i diritti e la libertà degli interessati; a.2) (E) che il DPO disponga di risorse sufficienti per svolgere i propri compiti.	Un impiego part-time per un DPO è accettabile a condizione che il tempo di lavoro assegnato sia sufficiente per consentire al DPO di svolgere i propri compiti.	Contratto del DPO. Documentazione della valutazione del tempo di lavoro del DPO.	38.2
G.9.3				**Compiti del responsabile della protezione dei dati**				**39**
G.9.3.1	CP	G	A	Compiti e mansioni del DPO	A) Il Richiedente deve dimostrare che sono stati assegnati i seguenti compiti al DPO: a.1) informare e consigliare il Richiedente e i suoi dipendenti coinvolti nel trattamento dei dati sui loro obblighi in materia di protezione dei dati; a.2) (E) monitorare i rischi e la conformità del trattamento dei dati con i regolamenti e le policy di protezione dei dati applicabili; a.3) (E) fornire consulenza sull'esecuzione della valutazione di impatto sulla protezione dei dati e monitorare le sue prestazioni (ai sensi dell'art. 35 del GDPR); a.4) (E) collaborare e fungere da punto di contatto con l'Autorità di Controllo; a.5) (E) gestire o controllare le richieste degli interessati nell'esercizio dei loro diritti.	Il Richiedente deve tenere un registro con: - il contratto di lavoro del DPO; - i compiti assegnati al DPO; - le comunicazioni con la DPA; - le attività del DPO; - le attività di formazione sulla protezione dei dati (frequentate e/o organizzate); - la valutazione dei rischi, DPIA, nonché audit sulla sicurezza e sulla protezione dei dati; - Le decisioni e le raccomandazioni del DPO (ove possibile).	Intervista del DPO. Contratto del DPO. Regole e policy.	39.1
G.9.3.2	CP	G	A	Obbligo di formazione del personale sulla protezione dei dati	A) Il Richiedente deve disporre di una policy, di regole o di una procedura per formare periodicamente il personale che ha accesso permanente o regolare ai dati personali.	Il Richiedente ha il dovere di garantire che il personale incaricato del trattamento dei dati personali abbia un'adeguata conoscenza e comprensione delle norme sulla protezione dei dati personali.	Intervista del DPO Documentazione e prove di formazione.	
G.10				**Trasferimenti di dati personali a paesi terzi o organizzazioni internazionali (se applicabile)** Obiettivo: Assicurare che in caso di trasferimento di dati personali relativi al Target of Evaluation verso paesi terzi o organizzazioni internazionali, tale trasferimento fornisca adeguate garanzie e salvaguardie agli interessati. Condizione: SE i dati personali nel Target of Evaluation vengono trasferiti a un paese terzo o a un'organizzazione internazionale, ALLORA:					
I trasferimenti di dati personali tra paesi appartenenti allo Spazio Economico Europeo non costituiscono trasferimenti verso paesi terzi.								
G.10.1				**Principi generali per i trasferimenti** Condizione: SE i dati trattati nel Target of Evaluation vengono trasferiti (o resi accessibili) a un paese terzo o a un'organizzazione internazionale, ALLORA:				**44**
G.10.1.1	CP	S	A	Convalida del trasferimento transfrontaliero verso paesi terzi	A) Il Richiedente deve avere una chiara mappatura o registrazione di tutti i trasferimenti di dati personali a paesi terzi e alle organizzazioni internazionali da parte del Target of Evaluation. E B) Il trasferimento dei dati personali deve essere stato valutato come lecito dal DPO o da un esperto legale con competenze adeguate, prendendo in considerazione: b.1) i rischi per le libertà e i diritti degli interessati; b.2) (E) le salvaguardie e le misure adottate per proteggere i dati trasferiti.	Il Richiedente deve disporre di regole, procedure o meccanismi per valutare e convalidare la conformità del trasferimento di dati personali a paesi terzi o a organizzazioni internazionali prima di autorizzare tali trasferimenti. Se i dati personali sono trasferiti per il trattamento in un paese terzo o a un'organizzazione internazionale, il Richiedente deve tenere una registro documentato con: - tutti i trattamenti dei dati che vengono effettuati in paesi terzi e/o da organizzazioni internazionali; - la valutazione della conformità di tale trasferimento; - la valutazione del rischio di compromettere il livello di protezione dei dati e/o di incidere sulle libertà e sui diritti degli interessati causato da tale trasferimento; - le salvaguardie, le misure tecniche e le misure organizzative messe in atto per proteggere i dati trasferiti. L'applicabilità della certificazione al trasferimento transfrontaliero di dati può essere soggetta a requisiti complementari.	Intervista del DPO. Dichiarazione scritta del DPO.	*44*

G.10.1.2	CP	S	A	Base giuridica del trasferimento transfrontaliero	SE i dati personali vengono trasferiti a paesi terzi o a organizzazioni internazionali, ALLORA si dovrà rispettare almeno una delle seguenti opzioni: A) Il paese terzo verso il quale vengono trasferiti i dati deve beneficiare di una decisione di adeguatezza. O B) Il trasferimento a un Paese terzo deve basarsi su salvaguardie adeguate e rispettare il criterio complementare G.10.1.3. O C) I dati sono trasferiti sulla base di norme vincolanti d'impresa (BCR) che sono state approvato dall'Autorità di Controllo del Richiedente. O D) Il trasferimento dei dati deve basarsi su deroghe per situazioni specifiche e rispettare il criterio complementare G.10.1.4.	Il Richiedente deve dimostrare che il trasferimento transfrontaliero dei dati è legittimo. Si noti che fornire l'accesso ai dati a un paese terzo equivale a un trasferimento verso tale paese. Un consenso valido deve essere conforme ai criteri G.1.2.1, G.2.1.2, G.2.1.3. Il GDPR richiede che la decisione di adeguatezza sia adottata e monitorata dalla Commissione europea (art. 45 GDPR). L'elenco delle decisioni di adeguatezza è pubblicato e aggiornato sul sito web della Commissione europea.	Revisione della documentazione. Intervista del DPO. Decisione di adeguatezza. Norme vincolanti d'impresa.	*44*
G.10.1.3				Trasferimento transfrontaliero basato su adeguate salvaguardie	SE i trasferimenti di dati personali a paesi terzi o a organizzazioni internazionali si basano su adeguate salvaguardie, ALLORA: A) Il Titolare o il Responsabile del trattamento nel paese terzo deve: a.1) verificare regolarmente la sicurezza della propria infrastruttura che tratta e/o conserva i dati del Target of Evaluation; a.2) (E) l'ultimo report di audit deve essere stato esaminato dal DPO del Richiedente e giudicato soddisfacente. E B) Il Titolare del trattamento o il Responsabile del trattamento nel paese terzo deve disporre di una procedura per consentire agli interessati di far valere i propri diritti e di accedere a rimedi legali efficaci da parte del Titolare o del Responsabile del trattamento situati nel paese terzo. E C) Il Richiedente deve fornire informazioni all'interessato su come esercitare i suoi diritti in relazione al trattamento dei suoi dati nei paesi terzi coinvolti nel trattamento. E D) Il DPO del Titolare del trattamento dovrà aver valutato e confermato che gli interessati possono esercitare efficacemente i loro diritti e accedere ai rimedi legali.	Il titolare del trattamento deve valutare l'adeguatezza e l'efficacia delle salvaguardie in vigore nel paese terzo o presso le organizzazioni internazionali (a seconda dei casi) prima di trasferire i dati personali.	Revisione della documentazione. Procedure, regole e policy. Intervista del DPO. Ispezione.	*46*
G.10.1.4				Trasferimento transfrontaliero basato su deroghe per situazioni specifiche	SE i dati personali sono trasferiti a paesi terzi o a organizzazioni internazionali sulla base di deroghe per situazioni specifiche, ALLORA: A) Il trasferimento si basa sul consenso quando: a.1) gli interessati devono aver dato un consenso esplicito e valido al trasferimento proposto; a.2) (E) gli interessati devono essere stati informati dei rischi per i loro diritti e libertà dovuti all'assenza di una decisione di adeguatezza e di salvaguardie appropriate. O B) La necessità del trasferimento dei dati deve essere valutata e stabilita per: b.1) l'esecuzione di un contratto concordato dall'interessato o l'attuazione di misure precontrattuali adottate su richiesta dell'interessato; b.2) (OPPURE) importanti motivi di interesse pubblico, fondati su una base giuridica riconosciuta nella giurisdizione del titolare del trattamento; b.3) (OPPURE) l'accertamento, l'esercizio o la difesa di diritti legali; b.4) (OPPURE) la tutela degli interessi vitali delle persone fisiche. O C) Il trasferimento deve essere effettuato da un registro pubblico: c.1) destinato a fornire informazioni al pubblico in base all'Unione o agli Stati membri legge; c.2) (E) aperto alla consultazione da parte del pubblico in generale o di chiunque possa dimostrare un interesse legittimo.	Il trasferimento transfrontaliero basato su deroghe per situazioni specifiche deve essere chiaramente documentato. Se il trasferimento si basa sul consenso della persona interessata, tale consenso deve essere informato e dato in modo chiaro ed esplicito dalla persona interessata dopo essere stata informata dei rischi connessi al trasferimento. La definizione e la portata della "deroga per situazioni specifiche" sono specificate nel regolamento. Il requisito c.2) è applicabile nella misura in cui sono soddisfatte le condizioni legali per la consultazione.	Revisione della documentazione. Procedure, regole e policy. Intervista del DPO. Ispezione.	*49*

G.10.1.5	CP	S	A	Valutazione complementare del rischio di trasferimento dei dati a paesi terzi senza decisione di adeguatezza	SE i dati personali trattati nell'ambito del Target of Evaluation vengono trasferiti a un paese terzo o a un'organizzazione internazionale senza una decisione di adeguatezza, ALLORA: A) Il Richiedente deve aver raccolto informazioni sulla normativa e sulla prassi del paese terzo in materia di protezione dei dati (e/o sull'organizzazione internazionale) al fine di valutare se: a.1) l'accesso e il trattamento da parte delle autorità del paese terzo si basano su regole chiare, precise e accessibili; a.2) (E) esistono meccanismi per rispettare e conformarsi ai principi di necessità e proporzionalità del trattamento dei dati; a.3) (E) l'autorità del Paese (e/o l'organizzazione internazionale) ha stabilito meccanismi di supervisione; a.4) (E) sono disponibili rimedi efficaci per le persone; a.5) (E) la legislazione sulla protezione dei dati è effettivamente applicata. E B) Il Richiedente deve avere: b.1) adottato misure per affrontare i rischi identificati e per portare il livello di protezione dei dati personali trasferiti al livello richiesto di equivalenza essenziale della protezione dei dati; b.2) (E) predisporre una procedura o una misura efficace per rivalutare i rischi connessi al trasferimento di dati personali a paesi terzi e a organizzazioni internazionali (in base al caso) su base regolare.	Il Richiedente deve verificare se i Paesi terzi coinvolti hanno adottato una normativa conforme alle Garanzie Essenziali Europee EDPB: 1 - l'accesso e il trattamento da parte delle autorità del paese terzo si basano su regole chiare, precise e accessibili; 2 - esistono meccanismi per il rispetto e l'osservanza dei principi di necessità e proporzionalità del trattamento dei dati; 3 - le autorità dei Paesi hanno stabilito meccanismi di supervisione; 4 - vengono messi a disposizione degli individui rimedi efficaci. Raccomandazioni EDPB 01/2020 sulle misure che integrano gli strumenti di trasferimento per garantire la conformità al livello di protezione dei dati personali dell'UE fornisce indicazioni chiare su come affrontare questo requisito: 1 "Conosci il tuo trasferimento" con una chiara mappatura del trasferimento dei dati (cfr. criterio G.10.1.1). 2 "Verifica lo strumento di trasferimento" per assicurarsi che sia adeguato (vedere i criteri G.10.1.2, G.10.1.3 e G.10.1.4). 3 "Valuta il paese terzo" e la sua legislazione e la prassi del paese terzo per determinare se la legislazione del paese terzo formalmente conforme agli standard dell'UE non è manifestamente applicata/conformata nella pratica e se esistono prassi incompatibili con gli impegni dello strumento di trasferimento in mancanza di una legislazione pertinente nel paese terzo. 4 "Identificare e adottare misure supplementari". Il Richiedente deve dimostrare che la sua decisione si basa su un'analisi efficace, che porta a individuare e adottare adeguate misure supplementari, come crittografia forte, pseudonimizzazione, trattamento suddiviso/multipartito, obbligo contrattuale di informazione (ad es. rapporti, "warrant canary", etc.). 5 "Adottare eventuali misure procedurali formali" in linea con le Raccomandazioni 01/2020. 6 "Rivalutare a intervalli appropriati il livello di protezione". Il Richiedente deve adottare un processo interno di rivalutazione annuale dei rischi legati al trasferimento di dati verso paesi terzi. Tale rivalutazione può essere integrata nella regolare policy di valutazione dei rischi.	Intervista del DPO. Documentazione sulla valutazione dei rischi e sulle misure adottate.	46
G.10.1.6	CP	S	A	Impegno del destinatario dei dati	SE i dati personali trattati nell'ambito del Target of Evaluation vengono trasferiti a un paese terzo o a un'organizzazione internazionale senza una decisione di adeguatezza, ALLORA: A) Il destinatario dei dati personali deve aver assunto impegni vincolanti ed esecutivi per l'applicazione di salvaguardie adeguate per la protezione dei dati trattati in relazione ai diritti degli interessati.	Come richiesto dall'Art. 42 del GDPR, i destinatari dei dati in paesi terzi dovrebbero essere vincolati da clausole contrattuali o altri strumenti giuridicamente vincolanti ad applicare salvaguardie adeguate, anche per quanto riguarda i diritti degli interessati. Ove applicabile, tale impegno può essere parte delle clausole contrattuali che vincolano il Titolare e il Responsabile del trattamento.	Intervista del DPO. Documentazione sulla valutazione dei rischi e sulle misure adottate.	42

G.10.2				Trasferimenti soggetti a salvaguardie adeguate Condizione: SE i dati trattati nell'ambito del Target of Evaluation vengono trasferiti a un paese terzo o a un'organizzazione internazionale sulla base di salvaguardie adeguate, ALLORA:			46
G.10.2.1	CP	S	A	Requisiti complementari per salvaguardie adeguate.	Il Richiedente deve dimostrare che il trasferimento dei dati beneficia di un'adeguata salvaguardia attraverso almeno uno dei seguenti meccanismi:	Le salvaguardie adeguate implicano che: - il Titolare e il Responsabile del trattamento hanno assunto impegni vincolanti e applicabili nel paese terzo; - tali impegni vincolanti ed esecutivi garantiscono l'applicazione di adeguate salvaguardie nelle operazioni di trattamento; - le salvaguardie appropriate contenute negli impegni vincolanti ed esecutivi si applicano anche a tutti i diritti degli interessati. - si è tenuto conto dell'impatto della legge nazionale e dello stato di diritto del Paese terzo.	Intervista del DPO. Documentazione sulle misure di salvaguardia fornite.	46.1. 46.2
				Autorità pubbliche	A) Il trasferimento dei dati ha salvaguardie adeguate grazie a uno strumento giuridicamente vincolante ed esecutivo tra autorità o enti pubblici.		*Strumento giuridicamente vincolante*	46.2.a
				Norme vincolanti d'impresa	O B) Il trasferimento dei dati ha salvaguardie adeguate grazie a norme vincolanti d'impresa approvate dall'Autorità di Controllo.	Le norme vincolanti d'impresa devono essere state approvate dall'Autorità di Controllo competente. Devono essere giuridicamente vincolanti e conferire diritti applicabili alle persone interessate.	*Norme vincolanti d'impresa. Corrispondenza con l'Autorità di Controllo*	46.2.b
				Clausola standard di protezione dei dati	O C) Il trasferimento dei dati ha salvaguardie adeguate grazie a clausole standard di protezione dei dati firmate congiuntamente dall'importatore e dall'esportatore.	Il GDPR prevede che le clausole contrattuali standard debbano essere adottate dalla Commissione Europea (ai sensi dell'art. 93(2) GDPR) o dall'Autorità di Controllo e approvate dalla Commissione Europea.	*Contratto.* *Pubblicazione delle clausole standard di protezione dei dati.*	46.2.c, 46.2.d
				Codice di condotta approvato	O D) Il trasferimento dei dati ha salvaguardie adeguate grazie a un codice di condotta approvato con l'impegno vincolante ed esecutivo di applicare le opportune salvaguardie.	Il GDPR richiede che il codice di condotta sia stato formalmente convalidato da un'Autorità di Controllo in conformità all'art. 40 del GDPR.	*Codice di condotta.*	46.2.e
				Certificazione	O E) Il trasferimento dei dati ha salvaguardie adeguate grazie a un meccanismo di certificazione, quando: e.1) il meccanismo di certificazione è approvato dall'autorità di protezione dei dati; e.2) (E) il Titolare o il Responsabile del trattamento nel paese terzo è vincolato da un impegno attuabile di applicare le opportune salvaguardie al trattamento dei dati, anche per quanto riguarda i diritti degli interessati.	Il GDPR richiede che un meccanismo di certificazione sia stato formalmente approvato ai sensi dell'articolo 42 del GDPR. L'elenco di tali schemi di certificazione approvati è pubblicato dall'EDPB.	*Documenti di certificazione e riferimenti.*	46.2.f
				Autorizzazione dell'Autorità di Controllo	O F) Il trasferimento dei dati è autorizzato dall'Autorità di Controllo sulla base di clausole contrattuali approvate con il Titolare o il Responsabile del trattamento.		*Autorizzazione dell'Autorità di Controllo.*	46.3
					O G) Il trasferimento dei dati è autorizzato dall'Autorità di Controllo sulla base di accordi amministrativi tra autorità o enti pubblici che comprendono: g.1) le disposizioni approvate dalle Autorità di Controllo; g.2) (E) disposizioni per garantire l'applicabilità e l'efficacia dei diritti degli interessati.		*Autorizzazione dell'Autorità di Controllo.*	46.3