C - ELENCO DELLE VERIFICHE E DEI CONTROLLI CONTESTUALI COMPLEMENTARI (CCC)

Org. di Cert.:
Richiedente:
Target of Evaluation
Nome (Esperto):
Data:

I seguenti criteri mirano ad affrontare i rischi tecnologici e specifici del settore legati al trattamento dei dati personali. Essi integrano i criteri fondamentali e devono essere applicati all'Target of Evaluation, se applicabile. 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.

Ref. ID	Richiedente	Specifico / Generico	Livello	TITOLO	CRITERI applicabili al Target of Evaluation (clausole prescrittive)	GUIDA ALL'ATTUAZIONE (clausole informative)	Mezzi di verifica suggeriti	GDPR
C				**Verifiche e controlli contestuali complementari**				
				Obiettivo:	Garantire che l'elaborazione dei dati nel Target of Evaluation sia conforme ai requisiti specifici del dominio e della tecnologia.			
C.1				**C Controlli complementari per siti web pubblici (ove applicabile)**				
				Condizione: SE il Target of Evaluation include un sito web accessibile al pubblico, ALLORA:				
L'uso dei cookie può essere soggetto a norme e linee guida complementari europee (ad es. ePrivacy) e nazionali che devono essere rispettate dal Richiedente.								
C.1.1.1	CP	S	A	HTTPS abilitato	A) L'HTTPS deve essere abilitato di default per l'accesso all'interfaccia web.	Il trasferimento dei dati tra l'interfaccia web e il server deve essere protetto.	Ispezione e test.	32
C.4				**C Videocamere e monitoraggio audio Controlli complementari (ove applicabile)**				
				Condizione: SE il Target of Evaluation include telecamere o monitoraggio audio, ALLORA:				
C.4.1.1	C	S	A	Convalida dell'installazione della telecamera da parte del responsabile della protezione dei dati	A) Il responsabile della protezione dei dati (DPO) o un esperto legale con competenze adeguate deve aver verificato e convalidato che l'utilizzo della videocamera non violi le leggi e le normative vigenti in materia di videosorveglianza, comprese le normative nazionali applicabili.	Il responsabile della protezione dei dati deve garantire che l'impiego della videocamera sia conforme alle leggi e ai regolamenti applicabili. Le normative nazionali spesso contengono disposizioni specifiche che specificano cosa può essere ripreso o meno attraverso la videosorveglianza.	Ispezione. Piano di installazione della videocamera e documentazione. Intervista con il responsabile della protezione dei dati (DPO). NOCAR report.	6

C.4.1.2	C	S	A	Informazioni sulla videosorveglianza	A) Il Richiedente deve comunicare agli interessati informazioni chiare sulle aree sottoposte a videosorveglianza attraverso: a.1) comunicazione scritta o notifica agli interessati se la videosorveglianza è limitata ad aree private il cui accesso è limitato e controllato; a.2) (OPPURE) una segnaletica visibile che informi l'interessato quando entra in tale area di sorveglianza.	È importante rendere gli interessati consapevoli della presenza della videosorveglianza. In aggiunta a queste opzioni, e anche per rendere più efficaci, il Comitato europeo per la protezione dei dati/EDPB promuove l'utilizzo di mezzi tecnologici per fornire informazioni agli interessati. Questo può includere, ad esempio, la geolocalizzazione delle telecamere e l'inclusione di informazioni in app o siti web di mappatura, in modo che le persone possano facilmente, da un lato, identificare e specificare le fonti video relative all'esercizio dei loro diritti e, dall'altro, ottenere informazioni più dettagliate sull'operazione di trattamento.	Ispezione. Documentazione. Intervista con il responsabile della protezione dei dati.	13
C.4.1.3	C	S	A	Sorveglianza dello spazio riservato ai client	SE le telecamere videosorvegliano spazi privati che ricevono visitatori o clienti ALLORA: A) Deve essere visibile l'informazione che nei locali viene effettuata la videosorveglianza.	Se le telecamere monitorano spazi privati che ricevono visitatori o clienti, allora il responsabile della protezione dei dati (DPO) deve assicurarsi che siano presenti informazioni visibili sul fatto che la videosorveglianza viene effettuata nei locali.	Ispezione.	13
C.4.1.4	C	S	A	Protezione della rete video	A) Le videocamere devono essere collegate: a.1) attraverso una rete proprietaria protetta da accessi non autorizzati da Internet; a.2) (OPPURE) attraverso connessioni criptate end-to-end (cioIPsec in modalità tunnel su IPv6).	La rete che collega le videocamere a il server che memorizza i dati deve essere adeguatamente protetto da accessi non autorizzati da parte di terzi.	Ispezione. Analisi del campione. Documentazione di rete.	32
C.4.1.5	C	S	A	Autenticazione di accesso alla telecamera	A) Le telecamere devono essere dotate di meccanismi di autenticazione per prevenire l'accesso non autorizzato con una password: a.1) maggiore o equivalente a 64 bit (~10 caratteri ASCII stampabili); a.2) (E) distinti per ciascuna telecamera; a.3) (E) mai simile alla password predefinita del produttore. O B) La telecamera deve essere collegata tramite una rete proprietaria a filo o a fibra ottica protetta da accessi non autorizzati da Internet.	Le videocamere devono essere efficacemente protetto da qualsiasi accesso non autorizzato.	Ispezione. Analisi del campione. Documentazione di configurazione.	25, 32
C.4.1.6	C	S	A	Limitazione dell'accesso al server video	A) L'accesso ai video memorizzati sul server deve: a.1) essere strettamente limitato ai dipendenti autorizzati con autenticazione individuale dell'accesso; a.2) (E) essere sistematicamente registrati.	L'accesso alle registrazioni video deve essere rigorosamente limitato. I dipendenti devono avere l'obbligo contrattuale di mantenere la riservatezza e/o la segretezza.	Ispezione. Analisi del campione. Registri di accesso.	25

C.5	C	Verifiche complementari per le implementazioni dell'Internet of Things (se applicabile) Condizione: SE il Target of Evaluation include implementazioni di Internet of Things (come sensori e attuatori) ALLORA:					
Nota Bene: Qualsiasi immagine, datibiometrici, ID utente, nonché i dati generati da dispositivi mobili IoT che possono seguire il movimento di persone fisiche o che possono rivelare informazioni sulle attività degli interessati (come i sensori di presenza o i contatori di energia) sono considerati dati personali.							
C.5.1	**C**	**Controlli e verifiche complementari per le implementazioni di Internet of Things**					
C.5.1.1	CP	S	A	Requisiti complementari della valutazione d'impatto	A) Il Richiedente deve aver eseguito una valutazione d'impatto sulla protezione dei dati (DPIA) che consideri i seguenti rischi complementari per i diritti e le libertà degli interessati: a.1) la diffusione dell'Internet of Things è stata violata e compromessa; a.2) (E) i dati IoT sono combinati con altri insiemi di dati che possono portare all'identificazione degli interessati.	Il GDPR richiede di eseguire la DPIA prima di utilizzando nuove tecnologie o il monitoraggio su larga scala dello spazio pubblico. Questo criterio integra il criterio G.8.	Report DPIA. Intervista alla Responsabile della Protezione dei Dati (DPO).	35
C.5.1.2	CP	S	A	Valutazione del rischio di vulnerabilità della rete IoT	A) Il Richiedente deve aver valutato i rischi associati alla rete IoT in termini di sicurezza, compreso il rischio che gli hacker utilizzino la rete IoT come punto di ingresso più debole per accedere ai server in cui sono memorizzati i dati personali.	La rete IoT offre un'ampia superficie di rischio e può soffrire di vincoli di sicurezza. Può essere utilizzati per hackerare la rete del Richiedente. Una valutazione del rischio e, se del caso, l'adozione di misure dovrebbero essere intraprese per prevenire l'uso dell'implementazione IoT per accedere ai server del Richiedente. Questo criterio integra i criteri G.6.3 e G6.2.5 e richiede di affrontare i rischi identificati.	Rapporto di valutazione dei rischi.	32
C.5.1.3	CP	S	A	Documentazione sull'implementazione IoT	A) Il Richiedente deve disporre di una documentazione aggiornata della propria implementazione IoT che includa: a.1) un inventario di tutti i dispositivi IoT installati con i loro singoli identificatori e la loro posizione; a.2) mappe di rete che comprendano tutte le IoT distribuite.	Il Richiedente deve tenere un registro completo documentazione della propria implementazione IoT. Deve sapere quali dispositivi IoT sono installati e dove. La descrizione tecnica degli elementi deve essere fornita ai revisori.	Revisione della documentazione.	30
C.5.1.4	CP	S	A	Aggiornamenti del firmware IoT	A) Il Richiedente deve disporre di una procedura o di un meccanismo per: a.1) monitorare la necessità di eseguire aggiornamenti sicuri del firmware e relative patch; a.2) (AND) aggiornare senza ritardi ingiustificati il firmware deprecato sui dispositivi IoT; a.3) (AND) utilizzare solo firmware da fonti affidabili per l'aggiornamento dei dispositivi IoT.	Le implementazioni IoT offrono un'ampia superficie di rischio. Il Richiedente deve assicurarsi che il firmware venga aggiornato regolarmente per neutralizzare qualsiasi vulnerabilità. Deve disporre di una procedura per monitorare la necessità di eseguire aggiornamenti e patch sicure del firmware per tutta la durata di vita del dispositivo.	Procedure e regole scritte. Ispezione. Test campione. Test di penetrazione.	32

C.5.1.5	CP	S	A	IoT encryption	A) La trasmissione di dati personali da parte dei dispositivi IoT deve essere criptata.	La trasmissione dei dati IoT deve essere crittografata per preservare la riservatezza dei dati personali in rete. La riservatezza dei dati personali che transitano tra un dispositivo e un servizio, in particolare i servizi associati, deve essere protetta con la crittografia delle migliori pratiche.	è necessario dimostrare che gli strumenti di crittografia sono utilizzati in conformità con la politica di crittografia/gestione delle chiavi.	32
C.5.1.6	CP	S	A	IoT access authentication	A) I nodi IoT devono utilizzare password o altri meccanismi di autenticazione.	I nodi IoT devono utilizzare un meccanismo di autenticazione per essere accessibili.	Test report. Ispezione	32
C.5.1.7	CP	S	A	Modifica delle password "di default"	A) I dispositivi IoT non devono mai utilizzare una password predefinita fornita dal produttore.	Le password in uso devono essere distinte dalle password predefinita fornita dal produttore. Le password utilizzate sui dispositivi IoT devono essere differire l'una dall'altra. Il dispositivodeve fornire all'utente un meccanismo facilmente accessibile e intuitivo per modificare il valore di autenticazione utilizzato.	Audit. Analisi del campione. Test di penetrazione.	32
C.5.1.8	CP	S	A	Least privileged principle	A) Deve esistere una politica di accesso restrittiva alla rete e ai dati IoT, conforme al principio dell'accesso "least privilege".	La configurazione della rete IoT e l'accesso ai dispositivi IoT devono essere ridotti al minimo e dovrebbero seguire il principio del minor privilegio limitando tutti gli accessi, le porte e le interfacce che non sono necessari.	Test di ispezione.	25, 32
C.5.2	**C Verifiche e controlli complementari per l'Internet of Things degli oggetti distribuiti in aree accessibili al pubblico**							
	Condizione: SE i dispositivi IoT sono distribuiti in aree accessibili al pubblico ALLORA:							
C.5.2.1	CP	S	A	Segnaletica per aree IoT	A) Le aree in cui i dispositivi IoT raccolgono dati personali nello spazio pubblico devono essere segnalate al pubblico.	Le aree in cui i dispositivi IoT raccolgono dati personali nello spazio pubblico devono essere chiaramente segnalate.	Verifica e controllo a campione della presenza di segnaletica accanto all'IoT o dove le persone interessate possono vederla.	13
C.5.2.2	CP	S	A	IoT transparent information	A) Gli interessati devono poter accedere facilmente a informazioni specifiche sui dispositivi IoT installati che raccolgono dati personali nello spazio pubblico, comprese le informazioni per contattare il responsabile della protezione dei dati.	Gli interessati devono poter accedere facilmente a informazioni sui dispositivi IoT che raccolgono dati personali nello spazio pubblico. Si possono utilizzare soluzioni come codici QR e/o applicazioni online e informazioni web (ad esempio privacyapp.info o applicazioni simili).	Ispezione. Test campione.	13

C.5.2.3	CP	S	B	Protezione fisica	A) I dispositivi IoT devono essere distribuiti in modo da ridurre al minimo il rischio di furto.	I dispositivi IoT devono essere protetti fisicamente contro il furto o l'accesso fisico per evitare l'hacking. I moti rubati possono essere utilizzati per testare e violare la sicurezza della rete IoT.	Ispezione.	32
C.5.2.4	CP	S	B	Resilience to outage	A) I dispositivi IoT devono essere resilienti a: a.1) interruzione di corrente; a.2) (E) interruzione della rete.	I dispositivi IoT devono essere in grado di riconnettersi in modo sicuro e di funzionare normalmente dopo un'interruzione di corrente. e/o interruzione della rete.	Ispezione. Test (togliendo temporaneamente l'alimentazione).	32
C.5.3	**C Verifiche e controlli complementari per l'IoT con categorie particolari di dati personali** Condizione: SE i dispositivi IoT elaborano categorie particolari di dati personali, come dati biometrici o datirelativi alla salute, ALLORA:							
C.5.3.1	CP	S	B	Affidabilità dell'autenticazione	A) Per impedire l'accesso non autorizzato, i meccanismi di autenticazione devono essere sufficientemente forti: a.1) una password di dimensioni maggiori o equivalenti a 80 bit (10 caratteri ASCII); a.2) (OPPURE) l'uso di IPsec in modalità tunnel su IPv6 tra il gateway della Personal Area Network e il server del Richiedente; a.3) (OPPURE) l'uso di un meccanismo di autenticazione che sia stato valutato da terze parti indipendenti come in grado di fornire un livello di affidabilità equivalente a quello di a.1; a.4) (OPPURE) l'uso di una rete proprietaria basata su fili o su fibra ottica che non abbia una connessione a Internet.	I meccanismi di autenticazione devono essere forti sufficiente a prevenire l'hacking. L'analisi del rischio che il dispositivo IoT di supporto possa essere violato e compromesso deve essere condotta da un esperto di cybersecurity. Per i dati biometrici o dati relativi alla salute, si dovrà perseguire un livello di garanzia più elevato, al fine di tenere conto del rischio più elevato per gli interessati.	Ispezione. Test e verifica dei campioni.	32

C.6				C Controlli complementari per le città intelligenti (dove applicabile) Condizione: SE il Target of Evaluation è legato alle infrastrutture delle Smart Cities, ALLORA:			Test e verifica dei campioni.	
C.6.1.1	CP	S	A	Coinvolgimento degli interessati nella DPIA	Il Richiedente deve aver coinvolto e consultato gli interessati nel processo di DPIA.	I progetti di Smart Ciry devono coinvolgere e consultare i cittadini nel processo di DPIA e affrontare le potenziali preoccupazioni che possono essere sollevato. Questo criterio integra i criteri G.8.	Report e documentazione DPIA.	35
C.6.1.2	CP	S	A	Informazioni agli interessati	Il Richiedente deve aver comunicato le finalità e i piani relativi al trattamento dei dati della smart city agli interessati locali.	I progetti Smart City devono essere comunicati alla popolazione locale con informazioni specifiche sulla politica di protezione dei dati.	Documentazione delle informazioni comunicate ai cittadini. Intervista al Responsabile della Protezione dei Dati (DPO). Intervista ai cittadini.	13
C.6.1.3	CP	S	A	Informazioni online sull'elaborazione dei dati IoT	Gli interessati avranno a disposizione informazioni online sulla strategia di implementazione della smart city, sulle finalità e sulle misure messe in atto per proteggere i dati personali.	È importante che le informazioni online a disposizione dei cittadini sulla smart city strategia di implementazione, lo scopo e la misure di protezione dei dati personali.	Ispezione del sito web.	13
C.6.1.4	CP	S	A	Informazioni sui dispositivi IoT	Il Richiedente dovrà fornire informazioni al pubblico sui dispositivi IoT installati nello spazio pubblico: a.1) aggiungere etichette come i QR code ai dispositivi IoT; a.2) (OPPURE) fornire informazioni online come un'applicazione mobile con una mappa che indichi la posizione dei dispositivi IoT.	Il Richiedente deve fornire informazioni pubbliche sui dispositivi IoT installati nello spazio pubblico in modo facilmente accessibile agli interessati. Dovrebbe essere preso in considerazione l'uso di etichette come QR code sui dispositivi IoT o informazioni online attraverso applicazioni mobili con una mappa che indichi la posizione dei dispositivi IoT.	Ispezione. Test di accesso alle informazioni in loco.	13
C.6.1.5	CP	S	A	Facilità di accesso alle informazioni del sito web	L'informativa sulla privacy e i dati di contatto del responsabile della protezione dei dati (DPO) devono essere accessibili con non più di tre clic dalla home page del sito web del Richiedente.	L'informativa sulla privacy e i dati di contatto del responsabile della protezione dei dati deve essere facilmente accessibile agli interessati dalla home page del sito web del Richiedente. Un buon approccio consiste nell'includere un link diretto all'informativa sulla privacy nella home page e nel piè di pagina delle pagine web.	Ispezione del sito web.	13

C.7	C	Verifiche complementari dei dati biometrici, medici e sanitari (se applicabile) Condizione: SE il Target of Evaluation comprende dati biometrici individuali, dati medici o dati relativi alla salute, ALLORA:					
Nota bene: qualsiasi dato che misuri caratteristiche fisiche, fisiologiche o comportamentali costituisce un dato biometrico.							
C.7.1.1	C	S	A	Valutazione d'impatto sulla protezione dei dati	A) Il Richiedente deve aver eseguito una Valutazione d'Impatto sulla Protezione dei Dati (DPIA).	A causa dell'elevato rischio intrinseco legato ai dati biometrici e dati relativi alla salute, è necessario eseguire una Valutazione dell'Impatto sulla Protezione dei Dati (DPIA). Questo criterio integra i criteri G.8.	Ispezione. Analisi del campione. Intervista al Responsabile della Protezione dei Dati (DPO).	32
C.7.1.2	C	S	B	Pseudonimizzazione	A) L'archiviazione dei dati biometrici e dei dati relativi alla salute deve essere protetta almeno dall'uso di tecniche di pseudonimizzazione o di crittografia (o di entrambe).	I dati personali biometrici, medici e relativi alla salute devono essere altamente protetti.	Ispezione. Analisi del campione. Intervista al DPO e al CISO.	25
C.7.1.3	C	S	B	Autenticazione mutifattoriale	A) L'accesso umano ai dati biometrici, medici e relativi alla salute richiede un meccanismo di autenticazione a più fattori.	I dati personali biometrici, medici e relativi alla salute devono essere altamente protetti.	Ispezione. Dimostrazione del controllo degli accessi.	32
C.7.1.4	C	S	B	Restrizioni alle applicazioni di tracciamento dei contatti	SE il Target of Evaluation include un'applicazione di tracciamento dei contatti, ALLORA: A) La richiesta deve: a.1) richiedere un'attivazione manuale da parte dell'utente per avviare l'elaborazione dei dati e la trasmissione degli identificativi; a.2) (AND) utilizzare identificatori pseudonimi; a.3) (AND) modificare automaticamente l'identificatore pseudonimizzato su base regolare. E B) L'utente deve essere in grado di: b.1) sapere se l'applicazione di tracciamento dei contatti è attiva o meno; b.2) (E) interrompere o sospendere la trasmissione del proprio identificatore.	Le applicazioni di tracciamento dei contatti comportano rischi specifici. Quando un utente viene diagnosticato come infetto, informazioni sulla sua precedente chiusura contatti o gli identificatori trasmessi dal sistema dell'applicazione dell'utente possono essere raccolti solo con il consenso di quest'ultimo. È necessario stabilire un metodo di verifica che permetta di affermare che la persona è effettivamente infetta senza identificare l'utente.	Ispezione. Test. Revisione della documentazione tecnica.	12, 25

C.8				**C Verifiche Complementari sul Processo Decisionale Automatizzato (se applicabile)** Condizione: SE il Target of Evaluation comprende un processo decisionale automatizzato che può avere un impatto sugli interessati, ALLORA:				
C.8.1.1	C	S	A	Test e analisi	A) L'algoritmo utilizzato per il processo decisionale automatizzato deve essere stato analizzato e testato per garantire che non produca risultati discriminatori, errati o ingiustificati.	Prima di utilizzare un algoritmo per la decisionale, l'algoritmo deve avere è stato analizzato e testato, preferibilmente da una terza parte, al fine di garantire che non produca risultati discriminatori, errati o ingiustificati.	Documentazione e rapporto di prova dell'algoritmo. Intervista al DPO, al CISO o ai dipendenti.	35
C.8.1.2	C	S	A	Documentazione scritta di terzi	SE l'algoritmo utilizzato è fornito da una terza parte ALLORA: A) Il Richiedente deve disporre di una documentazione del fornitore che comprenda: a.1) audit e test effettuati sull'algoritmo; a.2) (E) il risultato dei test che confermano che non sta producendo risultati discriminatori, errati o ingiustificati.	Se l'algoritmo utilizzato è fornito da una terza parte, quest'ultima deve fornire garanzie scritte che l'algoritmo è stato controllato e testato per garantire che non produca decisioni discriminatorie, errate o ingiustificate.	Documentazione sull'algoritmo. Intervista al Responsabile della Protezione dei Dati (DPO).	35
C.8.1.3	C	S	A	Diritto di ottenere spiegazioni sulle decisioni	Il Richiedente deve essere in grado di spiegare all'interessato le decisioni prese attraverso il processo decisionale automatizzato.	Le decisioni automatizzate rimangono sotto la responsabilità del Richiedente che deve essere in grado di spiegare all'interessato le ragioni della decisione.	Analisi del campione. Test. Documentazione sull'algoritmo. Intervista al Responsabile della Protezione dei Dati (DPO).	12, 13
C.8.1.4	C	S	A	Procedura per l'intervento umano	A) Il Richiedente deve disporre di regole, meccanismi o di una procedura che consentano l'intervento umano quando richiesto dall'interessato.	Il Richiedente ha l'obbligo di garantire un intervento umano nel processo decisionale su richiesta dell'interessato.	Procedura e regole. Intervista al DPO.	22
C.9				**C Verifiche complementari su Blockchain e Distributed Ledger Technology (se applicabile)** Condizione: SE il Target of Evaluation include l'uso di Blockchain o di qualsiasi Distributed Ledger Technology ALLORA:				
Nota bene: Blockchain è un'implementazione specifica della Distributed Ledger Technology (DLT).								
C.9.1.1	CP	S	A	Valutazione d'impatto sulla protezione dei dati	A) Deve essere stata eseguita una DPIA che abbia valutato i seguenti rischi complementari per i diritti e le libertà degli interessati: a.1) il rischio che la tecnologia impedisca all'interessato il diritto di rettificare o cancellare i propri dati; a.2) (E) il rischio che la tecnologia faccia trapelare dati personali a terzi non autorizzati.	La scelta di Blockchain / Distributed Ledger Technology deve essere documentata e giustificata con un'analisi e una descrizione del valore aggiunto dell'utilizzo di tale tecnologia. La DPIA deve documentare perché i rischi sono accettabile rispetto all'uso di altri tecnologie.	Documentazione sulla valutazione della Blockchain. Intervista al Responsabile della Protezione dei Dati (DPO).	25

C.9.1.2	CP	S	A	Conformità con l'esercizio effettivo dei diritti dell'interessato	A) L'utilizzo della tecnologia Blockchain / Distributed Ledger Technology non limiterà l'esercizio dei diritti di opposizione, rettifica e cancellazione dei dati personali degli interessati.	L'uso di Blockchain / Distributed Ledger Technologynon dovrebbe limitare l'esercizio dei diritti degli interessati di opporsi, rettificare e cancellare i propri dati personali. I meccanismi da prendere in considerazione includono la pseudonimizzazione (mantenendo l'identità dei dati degli interessati in un registro separato e modificabile, che consente di cancellare o modificare il record), l'uso di funzioni di hash crittografiche per preservare la identità dei soggetti interessati, l'utilizzo di standard avanzati come Next Generation Database Access Control (NDAC).	Ispezione. Test e dimostrazione dell'efficacia della capacità di attuazione dei diritti degli interessati.	16, 17, 21
C.9.1.3	CP	S	A	Crittografia	A) I dati personali memorizzati nella Blockchain / Distributed Ledger Technology saranno crittografati per ridurre il rischio di accesso da parte di terzi.	I dati personali memorizzati nella Blockchain / Distributed Ledger Technology dovrebbe essere crittografato per ridurre il rischio di un'azione di accesso non autorizzato da parte di terzi.	Ispezione. Verifica campionaria e controllo dei dataset. Intervista al CISO.	25, 32
C.9.1.4	CP	S	A	Verifica complementare e chiarimento delle responsabilità	A) Il Richiedente deve aver eseguito un'analisi complementare: a.1) chiarire i ruoli e le responsabilità di tutte le parti coinvolte nell'implementazione della Blockchain / Distributed Ledger Technology; a.2) (E) garantire che la Blockchain / Distributed Ledger Technology non trasferisca alcun dato personale del Target of Evaluation a terzi che non agiscano adeguatamente come responsabili del trattamento.	Con Blockchain / Distributed Ledger Technology, i dati archiviati sono in linea di principio condivisi e archiviati da terze parti. Ciò comporta il rischio elevato di perdere il controllo sulla conservazione e il controllo dell'accesso ai dati. Di conseguenza, i ruoli dei titolati del trattamento, dei contitolari del trattamento e del responsabile del trattamento devono essere chiaramente specificati e affrontati. La certificazione non può essere rilasciata il Target of Evaluation non è chiaramente stabilito e se l'accesso ai dati trattati non è effettivamente controllato dal Richiedente.	Ispezione. Verifica dei campioni e controllo delle serie di dati. Intervista al CISO.	25, 26, 33

C - Controlli e verifiche complementari contestuali e specifici del settore (CCC)

C.10				**C**	**Verifiche Complementari sulle soluzioni di anonimizzazione e pseudonimizzazione dei dati (se applicabili)**			
					Condizione: SE il Target of Evaluation è incentrato sul processo di anonimizzazione o pseudonimizzazione dei dati, ALLORA:			
C.10.1				**C**	**Anonimizzazione e rischio di reidentificazione**			
					Condizione: SE l'uso della tecnica di anonimizzazione è dichiarato dal Richiedente, ALLORA:			
Nota Bene: Solo i dati definitivamente anonimizzati e non più collegabili (direttamente o indirettamente) agli interessati possono essere considerati dati anonimizzati.								
C.10.1.1	CP	S	B	Valutazione dell'algoritmo	A) Il Richiedente deve disporre di un rapporto o di uno studio che dimostri che il processo e l'algoritmo utilizzati per l'anonimizzazione sono irreversibili. E B) La valutazione dell'irreversibilità dell'anonimizzazione deve tenere conto almeno dei seguenti rischi: b.1) per individuare singoli individui; b.2) (E) per collegare i record alle persone; b.3) (E) per dedurre informazioni sugli individui".	Il processo di anonimizzazione e l'algoritmo utilizzato devono essere matematicamente irreversibili (o riconosciuti/certificati come tali). Il rischio di reidentificazione indipendente di dati anonimizzati deve tenere conto del rischio di identificare un interessato in base a una combinazione di criteri specifici, in particolare se si tratta di dati granulari sull'età dell'interessato, sulla sua ubicazione o su attributi rari. L'analisi del rischio deve considerare: - il rischio di individuare singoli individui; - il rischio della capacità di collegamento; - il rischio di inferenza. Si raccomanda di consultare la raccomandazione 2014/05 del Comitato europeo per la protezione dei dati (EDPB).	Analisi di algoritmi e processi. Test di deanonimizzazione.	25, 32
C.10.1.2	CP	S	B	Verifica della deanonimizzazione	A) SE viene applicata la metodologia del Statistical Disclosure Control, ALLORA i set di dati anonimizzati devono essere coerenti e conformi alle soglie definite.	Dovrebbe essere impossibile deanonimizzare dati anonimizzati. Laddove le categorie particolari di dati personali sono rese anonime, si dovrà considerare un penetration test per deanonimizzare i dati anonimizzati.	Analisi del campione. Test di deanonimizzazione.	25, 32
C.10.2				**C**	**Pseudonimizzazione**			
					Condizione: SE l'uso della tecnica di pseudonimizzazione è dichiarato dal Richiedente, ALLORA:			
Nota Bene: Dal punto di vista legale, i dati pseudonimizzati devono essere trattati come dati personali e devono rispettare i relativi diritti e obblighi.								
C.10.2.1	CP	S	B	Dissociazione	A) Le informazioni necessarie per collegare gli interessati con i loro dati pseudonimizzati devono essere protette e conservate in modo sicuro con diritti di accesso distinti da quelli per gli insiemi dei dataset pseudonimizzati.	Le informazioni necessarie per la reidentificazione I dati pseudonimizzati dovrebbero essere protette e conservate in modo sicuro e con diritti di accesso diversi da quelli dei set dei dataset pseudonimizzati.	Verifica della posizione di archiviazione dei dati e dell'uso di diritti di accesso distinti.	25

C.10.2.2	CP	S	B	Limitazione dell'accesso	A) SE gli pseudo-identificatori sono generati utilizzando la crittografia, ALLORA le chiavi private devono essere protette. E B) SE gli pseudo-identificatori sono generati utilizzando una funzione di hashing, ALLORA devono essere adottate misure complementari, come la funzione salted-hash o la funzione keyed-hash.	L'accesso alle informazioni necessarie per la reidentificazione dei dati pseudonimizzati è strettamente limitato a coloro che hanno un accesso legittimo e ne hanno bisogno per svolgere il proprio lavoro.	Registro dei diritti di accesso. Verifica dell'efficacia della politica dei diritti di accesso. Intervista ai dipendenti e al Responsabile della Protezione dei Dati (DPO). Dichiarazione scritta del Responsabile della Protezione dei Dati (DPO).	25
C.10.2.3	CP	S	B	Conformità alla rettifica	SE il Richiedente può associare i dati pseudonimizzati agli interessati, ALLORA: A) La tecnica di pseudonimizzazione messa in atto non deve impedire l'esercizio dei diritti dell'interessato, tra cui: a.1) il diritto degli interessati di rettificare i propri dati pseudonimizzati; a.2) (E) il diritto degli interessati di cancellare i propri dati pseudonimizzati; a.3) (E) il diritto degli interessati di sospendere il trattamento dei loro dati pseudonimizzati.	I dati pseudonimizzati sono comunque dati personali e devono rispettare i diritti dell'interessato, compresi i diritti di rettifica, cancellazione e sospensione del trattamento. Nel caso in cui il Richiedente non sia in grado di identificare gli interessati associati a uno pseudonimo, i diritti degli individui saranno soddisfatti solo se questi ultimi forniscono informazioni aggiuntive per consentire al responsabile del trattamento di associarli al loro pseudonimo.	Ispezione e dimostrazione. Testare la procedura/meccanismo e controllare i risultati nel database.	16, 17, 18, 21

C.11 C Intelligenza artificiale e analisi dei dati - Controlli complementari (se applicabile)

Condizione: SE il Target of Evaluation comprende il trattamento dei dati personali basato sull'intelligenza artificiale o sull'analisi dei dati, ALLORA:

C.11.1 C Intelligenza artificiale

Condizione: SE l'obiettivo della valutazione comprende l'elaborazione di dati personali basati sull'intelligenza artificiale con un effetto potenziale sugli interessati, ALLORA:

Nota Bene: La Commissione Europea ha adottato la seguente definizione di Intelligenza Artificiale (IA) nella sua Comunicazione sull'IA: "*L'intelligenza artificiale (IA) si riferisce a sistemi che mostrano un comportamento intelligente analizzando il loro ambiente e intraprendendo azioni - con un certo grado di autonomia - per raggiungere obiettivi specifici. I sistemi basati sull'IA possono essere puramente software e agire nel mondo virtuale (ad esempio assistenti vocali, software di analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale) oppure l'IA può essere incorporata in dispositivi hardware (ad esempio robot avanzati, automobili autonome, droni o applicazioni dell' Internet of Things)". Una definizione complementare è stata elaborata da un gruppo di esperti di alto livello incaricato dall'UE: "I sistemi di intelligenza artificiale (IA) sono sistemi software (ed eventualmente anche hardware) progettati dall'uomo che, dato un obiettivo complesso, agiscono nella dimensione fisica o digitale percependo l'ambiente circostante attraverso l'acquisizione di dati, interpretando i dati strutturati o non strutturati raccolti, ragionando sulla conoscenza o elaborando le informazioni derivate da questi dati e decidendo le azioni migliori da intraprendere per raggiungere l'obiettivo prefissato". I sistemi di IA possono utilizzare regole simboliche o apprendere un modello numerico, e possono anche adattare il loro comportamento analizzando come l'ambiente è influenzato dalle loro azioni precedenti. Come disciplina scientifica, l'IA comprende diversi approcci e tecniche, come l'apprendimento automatico (di cui l'apprendimento profondo e l'apprendimento per rinforzo sono esempi specifici), il ragionamento automatico (che comprende la pianificazione, la programmazione, la rappresentazione e il ragionamento della conoscenza, la ricerca e l'ottimizzazione) e la robotica (che comprende il controllo, la percezione, i sensori e gli attuatori, nonché l'integrazione di tutte le altre tecniche nei sistemi cyber-fisici)*."

C - Controlli e verifiche complementari contestuali e specifici del settore (CCC)

C.11.1.1	CP	S	A	Valutazione complementare del rischio	A) Il Richiedente deve aver effettuato una Valutazione d'Impatto sulla Protezione dei Dati (DPIA) che comprenda i meccanismi di intelligenza artificiale utilizzati nel Target of Evaluation, tra cui a almeno la valutazione dei seguenti rischi: a.1) il rischio sul diritto alla vita privata degli interessati e alla protezione dei loro dati personali; a.2) (E) il rischio che vengano prese decisioni sulla base dell'IA che potrebbero avere un impatto negativo sull'interessato o limitare la sua libertà di decisione; a.3) (E) il rischio di ridurre la capacità dell'interessato di controllare l'uso dei propri dati personali; a.4) (E) il rischio che i dati e/o gli algoritmi possano essere manipolati; a.5) (E) il rischio che l'algoritmo di IA sia soggetto a pregiudizi o porti a decisioni discriminatorie o ingiuste; a.6) (E) il rischio che i dati personali vengano utilizzati per qualsiasi tipo di social scoring, soprattutto per quanto riguarda i social media e i servizi cloud; a.7) (E) il rischio che i dati personali vengano utilizzati dall'IA in modo intrusivo.	L'intelligenza artificiale può migliorare il benessere e apportare numerosi benefici. Tuttavia, è anche un'importante fonte di rischi e dovrebbe rimanere sotto il controllo delle persone interessate dal sistema di IA. Un sistema di IA può aiutare le persone interessate a prendere decisioni ottimali, ma le correlazioni di dati utilizzate dall'IA possono comportare una mancanza di trasparenza, di controllo umano, di responsabilità e di responsabilità percepite. Pertanto, gli interessati dovrebbero sempre avere la possibilità di annullare le decisioni prese dall'IA se queste hanno un impatto diretto su di loro.	Documentazione DPIA. Ispezione. Colloquio con il DPO e gli interessati.	35
C.11.1.2	CP	S	A	Consenso informato complementare	A) SE il trattamento è basato sul consenso, l'interessato deve essere stato informato in modo chiaro ed esplicito riguardo a: a.1) l'uso dell'intelligenza artificiale prima di raccogliere il loro consenso e trattare i loro dati; a.2) (E) le ragioni e lo scopo dell'utilizzo di meccanismi di intelligenza artificiale; a.3) (E) i principali benefici e rischi identificati nella DPIA; a.4) (E) SE il meccanismo di IA porta a decisioni o previsioni che possono riguardare gli interessati, ALLORA devono essere fornite informazioni agli interessati informazioni sulla procedura di accesso, opposizione e rettifica dei risultati del trattamento dei dati basato su algoritmi di IA.	L'intelligenza artificiale può migliorare il benessere e apportare numerosi benefici. Tuttavia, è anche un'importante fonte di rischi e dovrebbe rimanere sotto il controllo delle persone interessate dal sistema di IA. Un sistema di intelligenza artificiale può aiutare gli interessati a prendere decisioni ottimali. Tuttavia, gli interessati devono sempre avere la possibilità di annullare le decisioni prese dall'IA se queste hanno un impatto diretto su di loro.	Interfaccia utente e/o documenti contrattuali con l'interessato. Ispezione. Regole, politiche, procedure e meccanismi in atto. Analisi del campione. Verifica della procedura messa a disposizione degli interessati.	7

C.11.1.3	CP	S	B	Tenuta dei registri	SE il Richiedente fornisce la soluzione di intelligenza artificiale utilizzata nel Target of Evaluation, ALLORA: A) Il Richiedente deve conservare la documentazione relativa alla selezione e/o allo sviluppo dell'algoritmo utilizzato dalla sua intelligenza artificiale.	È importante essere in grado di spiegare come vengono trattati i dati personali. Ad esempio, se l'applicazione ha addestrato l'algoritmo con set di dati e se questi dati sono resi anonimi, il Richiedente deve conservare nei suoi archivi i set di dati utilizzati per addestrare l'algoritmo.	Revisione della documentazione. Analisi del campione. Intervista con il Responsabile della Protezione dei Dati (DPO)e/o con esperti.	
C.11.1.4	CP	G	B	Valutazione continua del rischio	A) Il Richiedente deve disporre di regole, politiche, procedure o meccanismi per garantire che i rischi legati all'uso di tecniche di intelligenza artificiale siano monitorati E B) Oltre ai rischi abituali, l'analisi dei rischi deve tenere conto del rischio di manipolazione dei dati o degli algoritmi.	Gli algoritmi di IA hanno la capacità di evolversi e di aumentare le loro capacità nel tempo. Di conseguenza, i rischi per le persone interessate possono cambiare e aumentare nel tempo. Gli algoritmi di intelligenza artificiale e di apprendimento automatico dovrebbero adottare un approccio di data protection by design e by default nella loro concezione. È quindi importante che il Richiedente rivaluti regolarmente i rischi della tecnologia di intelligenza artificiale utilizzata per gli interessati, in particolare quando sono coinvolte categorie particolati di dati personali.	Regole, politiche, procedure e meccanismi. Documentazione della valutazione dei rischi. Ispezione. Intervista con il Responsabile della Protezione dei Dati (DPO)..	35
C.11.2				**C Analisi dei Big Data** Condizione: SE il Target of Evaluation include tecnologie di Big Data Analytics O qualsiasi elaborazione di dati superiore a 1 petabyte di dati all'anno, ALLORA:				
Nota Bene: I Big Data sono definiti come insiemi di dati estremamente grandi che possono essere analizzati in modo computazionale per rivelare modelli, tendenze e associazioni, soprattutto in relazione al comportamento e alle interazioni umane. I Big Data sono caratterizzati da un grande volume, un'elevata velocità di elaborazione dei dati e una varietà di dati elaborati (la regola delle 3 V specificata da Gartner). Inoltre, nel contesto dell'Europrivacy, riteniamo che qualsiasi analisi dei dati che comprenda più di 1 petabyte di dati all'anno sia da considerarsi come Big Data Analytics.								
C.11.2.1	CP	S	A	Controllo di conformità complementare da parte del Responsabile della Protezione dei Dati (DPO).	A) Il Il Responsabile della Protezione dei Dati (DPO)o un esperto con competenze adeguate deve aver valutato i rischi di estrazione o generazione di categorie di dati personali che eccedono la finalità dichiarata. E B) Se sono state individuate misure di mitigazione, il Richiedente deve aver intrapreso azioni per attuarle.	La big data analytics può consentire l'estrazione di dati e profili personali che non sono evidenti agli interessati. Ciò comporta il rischio di trattare i dati personali al di là dello scopo concordato. Tale analisi può essere inclusa in un processo di DPIA.	Ispezione. Analisi del campione di dati. Intervista al Responsabile della Protezione dei Dati (DPO) e ai dipendenti. Ispezione dell'algoritmo. Revisione del rapporto DPIA.	6, 25

C.12				**C Controlli complementari sull'ambiente di lavoro e sulle relazioni (se applicabile)** Condizione: SE il Target of Evaluation è legato all'ambiente di lavoro o alla relazione, ALLORA:				
C.12.1				**C Ambiente di lavoro** Condizione: SE il Target of Evaluation riguarda l'ambiente di lavoro, ALLORA:				
C.12.1.1	CP	G	A	Portate il vostro dispositivo	A) Il Richiedente deve avere regole, politiche o clausole contrattuali scritte che vietino o inquadrino l'uso di dispositivi personali da parte dei dipendenti (politica "Bring Your Own Device").	Con il lavoro a distanza sempre più dipendenti tendono a utilizzare i propri dispositivi, tra cui laptop, smartphone, tablet e chiavette USB per il lavoro. L'uso di dispositivi personali in un ambiente professionale costituisce un rischio importante per il trattamento dei dati personali che deve essere chiaramente valutato e inquadrato dal Richiedente.	Regole, politiche, clausole contrattuali. Meccanismi predisposti (ad es. per limitare l'accesso alle porte USB). Ispezione. Analisi di campioni. Verifica della procedura messa a disposizione degli interessati. Intervista al DPO, al CISO e ai dipendenti.	32
C.12.1.2	CP	S	A	Dispositivi professionali	SE il Target of Evaluation comprende dispositivi portatili professionali messi a disposizione dei dipendenti, ALLORA: A) Il Richiedente deve avere regole scritte, politiche o clausole contrattuali che specifichino le regole (o il divieto) di utilizzo di tali dispositivi per uso personale, tra cui: a.1) se il dispositivo può essere utilizzato per uso personale; a.2) (E) se i dati memorizzati nel dispositivo sono accessibili al datore di lavoro; a.3) (E) se il dispositivo e il suo contenuto sono accessibili a terzi; a.4) (E) le regole di sicurezza e di accesso applicabili al dispositivo.	La fornitura di dispositivi mobili, come i computer portatili, ai dipendenti può esporre i dati personali memorizzati o accessibili attraverso il dispositivo all'accesso di terzi e a rischi aggiuntivi. Il potenziale uso personale di tali dispositivi deve essere inquadrato e chiarito al fine di proteggere i dati trattati da accessi o rischi illegali. Allo stesso modo, il Richiedente deve proteggere la privacy dei propri dipendenti ed evitare qualsiasi malinteso sull'ambito di accesso che il Richiedente mantiene sui dispositivi messi a disposizione dei dipendenti.	Regole, politiche, procedure e meccanismi stabiliti. Clausole contrattuali. Ispezione. Analisi del campione. Verifica della procedura messa a disposizione degli interessati. Intervista a DPO, CISO e dipendenti.	32
C.12.2				**C Rapporto di lavoro** Condizione: SE il Target of Evaluation riguarda il rapporto di lavoro, ALLORA:				
C.12.2.1	CP	S	A	Accesso e convalida del Responsabile della Protezione dei Dati (DPO)	A) Il Richiedente deve disporre di regole, politiche, procedure o meccanismi scritti per consentire ai dipendenti di contattare facilmente il Responsabile della Protezione dei Dati (DPO) per una questione relativa al trattamento dei dati personali. E B) Il Responsabile della Protezione dei Dati (DPO) o un esperto con adeguate competenze giuridiche deve aver valutato e convalidato la legittimità, la proporzionalità e l'adeguatezza dei dati dei dipendenti trattati nell'ambito del Target of Evaluation.	Il Responsabile della Protezione dei Dati (DPO) deve essere facilmente raggiungibile dal dipendenti, ad esempio attraverso un'apposita informazioni pubblicate su Intranet. Il la comunicazione con il Responsabile della Protezione dei Dati (DPO) dovrebbe essere vantaggiosa da un chiaro impegno del Richiedente a rispettare la riservatezza di tali comunicazione e interazione tra dipendenti e il Responsabile della Protezione dei Dati (DPO).	Regole, politiche, procedure e meccanismi stabiliti. Clausole contrattuali. Ispezione. Analisi del campione. Verifica della procedura messa a disposizione dei dipendenti. Intervista al DPO e ai dipendenti.	13

C.13			**C**	**Servizi finanziari e assicurativi Controlli complementari (se del caso)** Condizione: SE il Target of Evaluation è legato ai servizi finanziari e assicurativi, ALLORA:				
C.13.1			**C**	**Servizi finanziari e assicurativi**				
C.13.1.1	CP	S	A	Informazioni sull'Autorità di vigilanza	A) Ove richiesto dalla legislazione nazionale, il Richiedente deve dimostrare di aver informato e, ove richiesto, di aver ottenuto l'autorizzazione preventiva dalla propria Autorità di Vigilanza nazionale a fornire i servizi finanziari e/o assicurativi nel Target of Evaluation.	Diverse legislazioni nazionali hanno adottato regolamenti specifici per limitare il trattamento dei dati nel settore dei servizi finanziari, come la valutazione del merito creditizio.	Comunicazione con l'Autorità di Vigilanza nazionale. Intervista al Responsabile della Protezione dei Dati (DPO).	6
C.13.1.2	CP	S	A	Limitazione del trattamento dei dati	A) Il Richiedente deve disporre di politiche, processi o meccanismi per limitare i dati e le informazioni trattate nella valutazione della solidità finanziaria e del merito creditizio degli interessati.	La valutazione del merito creditizio consente di accedere a informazioni altamente private e possono avere un impatto importante sui soggetti interessati. Occorre prestare particolare attenzione a questo tipo di trattamento dei dati per garantire che sia chiaramente ridotto a quanto necessario e che non abbia un impatto su terzi.	Regole, politiche, procedure e meccanismi stabiliti. Ispezione. Analisi del campione. Intervista al Responsabile della Protezione dei Dati (DPO) e ai dipendenti.	25
C. 14				**Controlli complementari dei veicoli connessi (se applicabile)** Condizione: SE il Target of Evaluation include i veicoli connessi, ALLORA:				
C.14.1.1	CP	S	A	Informazioni o documentazione sul trattamento dei dati	A) Il conducente ha accesso alle seguenti informazioni sul trattamento dei dati del Target of Evaluation: a.1) l'ambito e la natura del trattamento dei dati personali; a.2) (E) la finalità del trattamento dei dati personali; a.3) (E) come controllare e disattivare il trattamento dei dati personali; a.4) (E) come accedere e cancellare i dati personali memorizzati; a.5) (E) come contattare il Responsabile della Protezione dei Dati (DPO) del Titolare del trattamento.	Le informazioni più importanti sui trattamento dei dati dovrebbero sempre essere messe a disposizione dal produttore in forma facilmente comprensibile nella documentazione del veicolo.	Revisione della documentazione. Ispezione. Test. Analisi del campione.	12, 13
C.14.1.2	CP	S	A	Comunicazione dei dati di utilizzo del veicolo	SE i dati di utilizzo vengono comunicati o raccolti in remoto dal veicolo, ALLORA: A) Deve essere previsto un meccanismo o una procedura per garantire che il consenso informato preventivo del proprietario del veicolo viene raccolto prima della trasmissione di tali dati di utilizzo.	I dati sull'utilizzo del veicolo forniscono informazioni sullo stile di guida o sulla distanza percorsa dall'interessato. Il consenso può essere ottenuto barrando una casella che non è preselezionato, oppure, se tecnicamente possibile, utilizzando un dispositivo fisico o logico a cui la persona può accedere dal veicolo.	Ispezione. Test e analisi dei campioni. Revisione della documentazione tecnica.	7

C - Controlli e verifiche complementari contestuali e specifici del settore (CCC)

C.14.1.3	CP	S	A	Elaborazione regolare dei dati di geolocalizzazione	SE i dati di geolocalizzazione sono comunicati o raccolti in remoto dal veicolo, ALLORA: A) Il Responsabile della Protezione dei Dati (DPO) o un esperto qualificato deve aver valutato e convalidato che: a.1) la granularità dei dati di geolocalizzazione recuperati non è più dettagliata di quanto necessario per raggiungere lo scopo del trattamento dei dati; a.2) (E) il periodo di conservazione dei dati di geolocalizzazione non è più lungo di quanto necessario per raggiungere lo scopo del trattamento dei dati. E B) Deve essere previsto un meccanismo o un processo: b.1) garantire che la finalità del trattamento dei dati di geolocalizzazione sia comunicata al conducente; b.2) (E) per consentire al conducente di disattivare il processo di geolocalizzazione dei dati. E C) L'interfaccia utente del veicolo deve visualizzare un'icona per informare l'interessato quando vengono i dati di geolocalizzazione sono oggetto di trattamento.	Raccolta dei dati di geolocalizzazione di un veicolo dovrebbero essere considerati dati personali, in quanto la posizione di un veicolo è naturalmente associato alla posizione del suo driver. Come di conseguenza, deve essere altamente protetto in quanto rivela le abitudini di vita degli interessati, il loro luogo di lavoro e di residenza, il loro centro di interesse ed eventualmente informazioni sensibili.	Ispezione. Test campione. Documentazione relativa all'effettiva implementazione delle misure di sicurezza.	12, 13, 25
C.14.1.4	CP	S	A	Trattamento speciale dei dati di geolocalizzazione in caso di furto	SE esiste un meccanismo che consente di localizzare un veicolo in caso di furto, ALLORA: A) L'attivazione e la disattivazione della geolocalizzazione remota del veicolo in caso di furto devono essere controllate dal proprietario del veicolo (o da un'autorità nazionale qualificata).	Il servizio antifurto non deve raccogliere continuamente dati di geolocalizzazione, ma solo quando l'interessato attiva il servizio.	Ispezione. Test e analisi dei campioni. Revisione della documentazione tecnica.	7, 25
C.14.1.5	CP	S	A	Tracciamento tramite tecnologia WiFi all'interno del veicolo	SE il veicolo è dotato di connettività Wi-Fi, ALLORA: A) Il conducente ha la possibilità di a.1) per impedire al sistema WiFi del veicolo di collegarsi a punti di accesso esterni; a.2) (E) per disattivare la raccolta e la memorizzazione degli indirizzi IP e MAC dei passeggeri.	I produttori di veicoli, grazie alla proliferazione delle interfacce di connessione a Internet, hanno la possibilità di offrire modelli che includono una connessione dati cellulare integrata e sono in grado di creare reti Wi-Fi, il che comporta maggiori rischi per la privacy degli interessati. Attraverso i veicoli, i soggetti interessati diventano emittenti continui e possono essere identificati e tracciati. Per evitare il tracciamento, i produttori dovrebbero inserire nel veicolo opzioni di opt-out.	Ispezione. Test e analisi dei campioni. Revisione della documentazione tecnica.	25

C - Controlli e verifiche complementari contestuali e specifici del settore (CCC)

C.14.1.6	CP	S	A	Applicazioni ed elaborazione in auto	SE il Richiedente utilizza una piattaforma applicativa per auto, ALLORA: A) Dovrebbe esistere un meccanismo: a.1) informare i conducenti sui trattamenti didati personali dalle applicazioni in-car; a.2) (E) per consentire ai conducenti di attivare e disattivare il trattamento dei dati personali da parte delle applicazioni di bordo. E B) I dati personali raccolti dalle applicazioni in-car non saranno trasmessi a terzi, a meno che il conducente non abbia dato un consenso informato specifico. E C) Deve essere previsto un meccanismo che consenta al proprietario dell'autovettura: c.1) avere accesso ai dati personali generati dalle applicazioni in-car; c.2) (E) cancellare i dati personali raccolti dal veicolo prima della sua messa in vendita.	Garantire che i dati personali siano trattati internamente al veicolo garantisce agli interessati il controllo esclusivo e completo dei loro dati, presentando al contempo minori rischi per la privacy grazie al divieto di trattamento dei dati da parte di soggetti interessati all'insaputa dell'interessato.	Ispezione. Test campione. Analisi del sistema.	7, 12, 15, 17
C.14.1.7	CP	S	A	Monitoraggio comportamentale	SE i dati comportamentali vengono raccolti dal veicolo (ad esempio attraverso una scatola telematica), ALLORA: A) Il conducente deve essere specificamente informato su: a.1) la presenza di un monitoraggio comportamentale; a.2) (E) lo scopo e la portata del monitoraggio comportamentale. E B) I dati grezzi del comportamento di guida devono essere elaborati o pre-elaborati localmente (nel veicolo o sul dispositivo personale del conducente) per ridurre al minimo l'esposizione dei dati.	La raccolta e l'elaborazione di informazioni comportamentali costituisce un'importante fonte di rischio per gli interessati. Il Richiedente ha la responsabilità di garantire la sicurezza dei dati raccolti (ad esempio, attraverso la telematics box), al fine di evitare che i dati vengano utilizzati in modo improprio sulla base della creazione del profilo di movimento del conducente.	Ispezione. Analisi del sistema. Test campione. Revisione della documentazione tecnica.	25

C - Controlli e verifiche complementari contestuali e specifici del settore (CCC)

C.14.1.8	CP	S	A	Requisiti di utilizzo del sistema eCall	SE un sistema eCall è incluso nel Target of Evaluation, ALLORA: A) Il Richiedente deve garantire che agli interessati vengano fornite informazioni su: a.1) l'ambito e le finalità del trattamento dei dati da parte di eCall; a.2) (E) il periodo di conservazione dei dati memorizzati dal sistema eCall; a.3) (E) il fatto che il veicolo non sia costantemente sorvegliato; a.4) (E) il fatto che il sistema eCall sia attivato di default; a.5) (E) il contatto competente per presentare una richiesta ed esercitare i diritti dell'interessato.	Il sistema eCall permette ai conducenti in Europa di chiamare automaticamente i servizi di emergenza locali in caso di incidente. I manuali d'uso e i produttori devono fornire informazioni chiare e complete sull'elaborazione dei dati tramite il sistema eCall.	Revisione della documentazione. Ispezione. Test.	12, 13
C.14.1.9	CP	S	A	Protezione delle comunicazioni del veicolo	A) Il sistema di comunicazione del veicolo deve: a.1) criptare i canali di comunicazione; a.2) (E) utilizzare il meccanismo di autenticazione dei dispositivi che partecipano alla comunicazione con il veicolo; a.3) (E) utilizzare il meccanismo di autenticazione dei server autorizzati a eseguire patch e aggiornamenti firmware/software; a.4) (E) se applicabile, l'uso delle frequenze assegnate alla comunicazione con i veicoli.	Il Richiedente ha l'obbligo di adottare misure per garantire la riservatezza dei dati personali all'interno del veicolo e dei dati trasmessi fuori dal veicolo, evitando la divulgazione a terzi non autorizzati. Di conseguenza, la riservatezza e la sicurezza dei dati devono essere applicate ai dati elaborati e raccolti all'interno del veicolo e ai dati trasmessi fuori dal veicolo. Le misure di sicurezza per il sistema di comunicazione del veicolo devono essere adeguate ai rischi posti dal trattamento dei dati e devono essere regolarmente riviste e aggiornate.	Relazione e documentazione sull'analisi dei rischi. Ispezione. Test.	32

C - Controlli e verifiche complementari contestuali e specifici del settore (CCC)

C.14.1.10	CP	S	A	Altre misure di sicurezza	A) L'auto deve includere le seguenti misure di sicurezza: a.1) deve separare le funzioni vitali del veicolo da quelle che dipendono dalle capacità di telecomunicazione; a.2) (E) richiede l'autenticazione dell'utente per accedere ai dati personali memorizzati; a.3) (E) deve includere un sistema o una soluzione per rilevare e avvisare in caso di intrusioni nel sistema di gestione dei dati del veicolo. a.2) (E) deve consentire il patching remoto delle vulnerabilità del firmware e del software durante la vita del veicolo; a.5) (E) deve memorizzare una cronologia degli accessi al sistema informativo del veicolo.	Il fornitore di servizi deve essere in grado di mettere misure che garantiscano la sicurezza e la riservatezza del trattamento dei dati e devono prendere tutte le precauzioni necessarie per impedire che il controllo venga effettuato da una persona non autorizzata. Le misure adottate devono essere adeguate al livello di sensibilità dei dati.	Revisione della documentazione delle misure di sicurezza e delle specifiche tecniche. Ispezione. Test campione. Analisi del sistema.	32
C.14.1.11	CP	S	B	Restrizioni ai dati biometrici	SE i dati biometrici vengono utilizzati nei veicoli connessi ALLORA: A) L'interessato deve poter utilizzare un'alternativa non biometrica. E B) I dati biometrici: b.1) non deve essere trasmesso a un server remoto; b.2) (E) non deve essere memorizzato in chiaro. E C) Il rischio connesso all'uso di dati biometrici nel trattamento deve essere stato valutato nel contesto di una valutazione d'impatto sulla protezione dei dati (DPIA).	Il Richiedente deve garantire che i dati biometrici siano protetti da accessi non autorizzati. In particolare, i dati biometrici non devono essere memorizzati in formato grezzo, ma devono utilizzare funzioni crittografiche (ad es. funzione hash) o altre soluzioni simili.	Ispezione. Test campione. Analisi del sistema.	9
C.14.1.12	CP	S	B	Elaborazione di dati che rivelano reati o altre infrazioni	A) La valutazione dell'impatto del trattamento dei dati (DPIA) deve aver valutato il rischio per gli interessati che il trattamento dei dati del veicolo comunichi reati o altre infrazioni.	I dati personali che si riferiscono a potenziali reati penali devono essere trattati a livello locale se l'interessato ha il pieno controllo sul trattamento. Questo criterio integra il criterio G.8.	Valutazione dell'impatto sulla protezione dei dati (DPIA) e/o rapporti di analisi dei rischi.	10

C.14.1.13	CP	S	B	Protezione del traffico V2X e dei dati di comunicazione	SE le comunicazioni V2X sono implementate, ALLORA: A) Il Richiedente deve disporre di regole, politiche, clausole contrattuali, linee guida o meccanismi per garantire che l'elaborazione dei dati sul traffico sia eseguita solo da entità o fornitori di servizi autorizzati. E B) Il richiedente deve attuare misure tecniche per: b.1) impedire l'identificazione o la reidentificazione di veicoli o utenti; b.2) (E) ridurre la divulgazione delle informazioni al minimo indispensabile per il funzionamento del sistema; b.3) (E) impedire il collegamento dei diversi pseudonimi assegnati a un veicolo; b.4) (E) garantire che la revoca delle credenziali non influisca sulla non collegabilità dei messaggi precedentemente firmati.	I dati di traffico e comunicazione devono essere elaborati solo dall'entità V2X/fornitore di rete. È necessario implementare procedure quali l'anonimizzazione e la pseudonimizzazione per garantire la non identificabilità, la divulgazione minima, la non collegabilità e la privacy in avanti e indietro.	Revisione della documentazione. Ispezione. Test e analisi dei campioni.	32
C.15				**C Controlli complementari su Smart Grid e Metering (se applicabile)** Condizione: SE il Target of Evaluation include smart grid o smart metering ALLORA:				
C.15.1.1	CP	S	A	Estensione della DPIA	A) Il Richiedente deve aver effettuato una Valutazione d'Impatto sulla Protezione dei Dati (DPIA) che abbia tenuto conto almeno di: a.1) il rischio di profilazione dell'interessato e di sorveglianza di massa; a.2) (E) il rischio di accesso di terzi; a.3) (E) il rischio di hackeraggio dei contatori intelligenti; a.4) (E) l'impatto sul rischio degli intervalli di misurazione previsti. E B) Il Richiedente deve aver adottato misure per affrontare i rischi identificati dalla DPIA.	La misurazione intelligente può rivelare un'ampia serie di dati personali, compresi i modelli comportamentali e pratiche religiose (ad esempio digiuni e celebrazioni religiose). Si noti che l'EDPB fornisce un modello di DPIA dedicato ai contatori intelligenti. Questo criterio integra i criteri G.8.	Revisione della documentazione DPIA. Intervista al Responsabile della Protezione dei Dati (DPO).	35

C - Controlli e verifiche complementari contestuali e specifici del settore (CCC)

C.15.1.2	CP	S	A	Minimizzazione dei dati by design	A) Il Responsabile della Protezione dei Dati (DPO) o un esperto qualificato deve aver valutato e concluso che: a.1) i contatori intelligenti trasmettono solo i dati necessari per raggiungere lo scopo del trattamento dei dati; a.2) (E) ove applicabile, i dati sono trattati e/o aggregati a livello locale per evitare un inutile trasferimento di dati personali; a.3) (E) l'accesso ai dati trattati è strettamente limitato ai soggetti e agli utenti che hanno legittimamente bisogno di accedervi; a.4) (E) il periodo di conservazione dei dati è limitato e giustificato.	Le smart grid e gli smart metering possono raccogliere e generare informazioni molto dettagliate e ricche. È estremamente importante garantire che l'elaborazione dei dati sia conforme ai principi della minimizzazione dei dati e della protezione dei dati by design. Questo criterio è complementare ai criteri G.6.1.	Revisione della documentazione. Intervista al Responsabile della Protezione dei Dati (DPO).	25
C.15.1.3	CP	S	A	Privacy Enhancing Technologies (PET)	A) Il Richiedente deve: a.1) criptare le comunicazioni remote con gli smart meter; a.2) (E) pseudonimizzare gli identificativi degli interessati; a.3) (E) ha analizzato e valutato l'applicabilità di altre tecnologie di miglioramento della privacy (PET), come i protocolli di mascheramento e l'aggregazione dei dati.	Le tecnologie di miglioramento della privacy (PET) devono essere utilizzato come adeguato per ridurre al minimo il rischio per gli interessati.	Ispezione. Colloquio con il DPO e/o il CISO. Analisi del campione. Revisione della documentazione tecnica.	25, 32
C.15.1.4	CP	S	A	Edge processing by default	A) Ove applicabile, i contatori intelligenti devono evitare di trasmettere dati che possono essere elaborati o aggregati localmente.	L'edge processing dei dati presenta diversi vantaggi, tra cui la riduzione al minimo dei dati personali da trasferire in rete.	Ispezione. Colloquio con il DPO e/o il CISO. Analisi del campione. Revisione della documentazione tecnica.	25
C.15.1.5	CP	S	A	Requisiti di sicurezza complementari alle smart grid	A) Il Richiedente deve implementare misure tecniche e organizzative complementari per proteggere la rete smart grid e il trattamento di dati, tra cui: a.1) incorporare meccanismi di autenticazione nei contatori intelligenti per riservare l'accesso remoto solo ai sistemi e agli utenti autorizzati; a.2) (E) per preservare l'integrità dei dati da modifiche non autorizzate; a.3) (E) per abilitare la sicurezza delle patch e degli aggiornamenti del firmware in remoto.	I contatori intelligenti hanno una lunga aspettativa di vita pertanto adeguate misure di sicurezza devono essere implementati, aggiornati e migliorati nel tempo e devono essere regolarmente sottoposti a revisione e test.	Ispezione. Colloquio con il DPO e/o il CISO. Analisi del campione. Revisione della documentazione tecnica.	32

C.15.1.6	CP	S	A	Disattivazione degli Smart meters	SE i contatori intelligenti memorizzano i dati di consumo, ALLORA: A) Il Richiedente deve disporre di una procedura o di un meccanismo per garantire che i dati memorizzati vengano sistematicamente cancellati nei contatori intelligenti che vengono dismessi.	C'è il rischio che i contatori dismessi tenere traccia dei precedenti dati di consumo dell'interessato precedente. Una procedura chiara dovrebbe essere stabilito dal Richiedente per sistematicamente pulire la memoria dei contatori dismessi.	Ispezione. Colloquio con il DPO e/o il CISO. Analisi del campione. Revisione della documentazione delle politiche e delle procedure.	25
C.50				**C Verifiche complementari del settore pubblico (se applicabile)** Condizione: SE il Richiedente è un ente del settore pubblico ALLORA:				
Nota bene: il settore pubblico comprende le organizzazioni che sono sotto l'autorità e il controllo effettivo delle autorità pubbliche.								
C.50.1				**C Requisiti generali del settore pubblico**				
C.50.1.1	CP	S	A	Limitazione dell'interesse legittimo	A) La liceità del trattamento dei dati non deve basarsi su una rivendicazione di interesse legittimo di cui all'art. 6 del GDPR nello svolgimento delle mansioni del Richiedente. 6 nello svolgimento dei compiti del Richiedente.	Ai sensi dell'art. 6.1 del GDPR, il legittimo interesse non può essere utilizzato dalle autorità pubbliche come base di legittimità per il trattamento dei dati.	Comunicazione con l'Autorità di Vigilanza nazionale. Intervista al Responsabile della Protezione dei Dati (DPO).	6.1
C.50.1.2	CP	S	A	Restrizioni al trasferimento transfrontaliero dei dati	SE il Target of Evaluation include il potenziale trasferimento di dati personali a paesi terzi che non hanno una decisione di adeguatezza e non forniscono garanzie adeguate per i diritti e le libertà degli interessati, ALLORA: A) Il Richiedente deve avere politiche, regole o meccanismi in atto per prevenire tale trasferimento nello svolgimento del suo compito sulla base di: a.1) il consenso dell'interessato; a.2) (E) l'esecuzione di un contratto con o a beneficio dell'Interessato.	L'Art. 49 limita l'applicabilità del consenso e dell'esecuzione del contratto per gli enti pubblici in caso di trasferimento di dati personali verso paesi terzi che non garantiscono un'adeguata protezione dei dati personali.	Revisione della documentazione delle politiche. Ispezione. Analisi del campione. Intervista con il Responsabile della Protezione dei Dati (DPO).	49