*ALLEGATO*

**Clausole contrattuali tipo**

SEZIONE I

*Clausola 1*

***Scopo e ambito di applicazione***

a) Scopo delle presenti clausole contrattuali tipo (di seguito «clausole») è garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

b) I titolari del trattamento e i responsabili del trattamento di cui all'allegato I hanno accettato le presenti clausole al fine di garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 e/o dell'articolo 29, paragrafi 3 e 4, del regolamento (UE) 2018/1725.

c) Le presenti clausole si applicano al trattamento dei dati personali specificato all'allegato II.

d) Gli allegati da I a IV costituiscono parte integrante delle clausole.

e) Le presenti clausole lasciano impregiudicati gli obblighi cui è soggetto il titolare del trattamento a norma del regolamento (UE) 2016/679 e/o del regolamento (UE) 2018/1725.

f) Le presenti clausole non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo V del regolamento (UE) 2016/679 o del regolamento (UE) 2018/1725.

*Clausola 2*

***Invariabilità delle clausole***

a) Le parti si impegnano a non modificare le clausole se non per aggiungere o aggiornare informazioni negli allegati.

b) Ciò non impedisce alle parti di includere le clausole contrattuali tipo stabilite nelle presenti clausole in un contratto più ampio o di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti clausole o ledano i diritti o le libertà fondamentali degli interessati.

*Clausola 3*

***Interpretazione***

a) Quando le presenti clausole utilizzano i termini definiti, rispettivamente, nel regolamento (UE) 2016/679 o nel regolamento (UE) 2018/1725, tali termini hanno lo stesso significato di cui al regolamento interessato.

b) Le presenti clausole vanno lette e interpretate alla luce delle disposizioni del regolamento (UE) 2016/679 o del regolamento (UE) 2018/1725, rispettivamente.

c) Le presenti clausole non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal regolamento (UE) 2016/679 / dal regolamento (UE) 2018/1725, o che pregiudichi i diritti o le libertà fondamentali degli interessati.

*Clausola 4****Gerarchia***

In caso di contraddizione tra le presenti clausole e le disposizioni di accordi correlati, vigenti tra le parti al momento dell'accettazione delle presenti clausole, o conclusi successivamente, prevalgono le presenti clausole.

*Clausola 5 — Facoltativa*

***Clausola di adesione successiva***

a) Qualunque entità che non sia parte delle presenti clausole può, con l'accordo di tutte le parti, aderire alle presenti clausole in qualunque momento, in qualità di titolare del trattamento o di responsabile del trattamento, compilando gli allegati e firmando l'allegato I.

b) Una volta compilati e firmati gli allegati di cui alla lettera a), l'entità aderente è considerata parte delle presenti clausole e ha i diritti e gli obblighi di un titolare del trattamento o di un responsabile del trattamento, conformemente alla sua designazione nell'allegato I.

c) L'entità aderente non ha diritti od obblighi derivanti a norma delle presenti clausole per il periodo precedente all'adesione.

SEZIONE II

**OBBLIGHI DELLE PARTI**

*Clausola 6*

***Descrizione del trattamento***

I dettagli dei trattamenti, in particolare le categorie di dati personali e le finalità del trattamento per le quali i dati personali sono trattati per conto del titolare del trattamento, sono specificati nell'allegato II.

*Clausola 7*

***Obblighi delle parti***

7.1. **Istruzioni**

a) Il responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento. In tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. Il titolare del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate.

b) Il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, le istruzioni del titolare del trattamento violino il regolamento (UE) 2016/679/ il regolamento (UE) 2018/1725 o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei dati.

7.2. **Limitazione delle finalità**

Il responsabile del trattamento tratta i dati personali soltanto per le finalità specifiche del trattamento di cui all'allegato II, salvo ulteriori istruzioni del titolare del trattamento.

7.3. **Durata del trattamento dei dati personali**

Il responsabile del trattamento tratta i dati personali soltanto per la durata specificata nell’allegato II.

7.4. **Sicurezza del trattamento**

a) Il responsabile del trattamento mette in atto almeno le misure tecniche e organizzative specificate nell’allegato III per garantire la sicurezza dei dati personali. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati (violazione dei dati personali). Nel valutare l’adeguato livello di sicurezza, le parti tengono debitamente conto dello stato dell’arte, dei costi di attuazione, nonchè della natura, dell’ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati.

b) Il responsabile del trattamento concede l'accesso ai dati personali oggetto di trattamento ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Il responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

7.5. **Dati sensibili**

Se il trattamento riguarda dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose, filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati («dati sensibili»), il responsabile del trattamento applica limitazioni specifiche e/o garanzie supplementari.

7.6. **Documentazione e rispetto**

a) Le parti devono essere in grado di dimostrare il rispetto delle presenti clausole.

b) Il responsabile del trattamento risponde prontamente e adeguatamente alle richieste di informazioni del titolare del trattamento relative al trattamento dei dati conformemente alle presenti clausole.

c) Il responsabile del trattamento mette a disposizione del titolare del trattamento tutte le informazioni necessarie a dimostrare il rispetto degli obblighi stabiliti nelle presenti clausole e che derivano direttamente dal regolamento (UE) 2016/679 e/o dal regolamento (UE) 2018/1725. Su richiesta del titolare del trattamento, il responsabile del trattamento consente e contribuisce alle attività di revisione delle attività di trattamento di cui alle presenti clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito a un riesame o a un'attività di revisione, il titolare del trattamento può tenere conto delle pertinenti certificazioni in possesso del responsabile del trattamento.

d) Il titolare del trattamento può scegliere di condurre l'attività di revisione autonomamente o incaricare un revisore indipendente. Le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del responsabile del trattamento e, se del caso, sono effettuate con un preavviso ragionevole.

e) Su richiesta, le parti mettono a disposizione della o delle autorità di controllo competenti le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di revisione.

7.7. **Ricorso a sub-responsabili del trattamento**

a) OPZIONE 1: AUTORIZZAZIONE PRELIMINARE SPECIFICA: Il responsabile del trattamento non può subcontrattare a un sub-responsabile del trattamento i trattamenti da effettuare per conto del titolare del trattamento conformemente alle presenti clausole senza la previa autorizzazione specifica scritta del titolare del trattamento. Il responsabile del trattamento presenta la richiesta di autorizzazione specifica almeno [SPECIFICARE IL PERIODO] prima di ricorrere al sub-responsabile del trattamento in questione, unitamente alle informazioni necessarie per consentire al titolare del trattamento di decidere in merito all'autorizzazione. L'elenco dei sub-responsabili del trattamento autorizzati dal titolare del trattamento figura nell'allegato IV. Le parti tengono aggiornato tale allegato.

OPZIONE 2: AUTORIZZAZIONE SCRITTA GENERALE: Il responsabile del trattamento ha l'autorizzazione generale del titolare del trattamento per ricorrere a sub-responsabili del trattamento sulla base di un elenco concordato. Il responsabile del trattamento informa specificamente per iscritto il titolare del trattamento di eventuali modifiche previste di tale elenco riguardanti l'aggiunta o la sostituzione di sub-responsabili del trattamento con un anticipo di almeno [SPECIFICARE IL PERIODO], dando così al titolare del trattamento tempo sufficiente per poter opporsi a tali modifiche prima del ricorso ai sub-responsabili del trattamento in questione. Il responsabile del trattamento fornisce al titolare del trattamento le informazioni necessarie per consentirgli di esercitare il diritto di opposizione.

b) Qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del responsabile del trattamento), stipula un contratto che impone al sub-responsabile del trattamento, nella sostanza, gli stessi obblighi in materia di protezione dei dati imposti al responsabile del trattamento conformemente alle presenti clausole. Il responsabile del trattamento si assicura che il sub-responsabile del trattamento rispetti gli obblighi cui il responsabile del trattamento è soggetto a norma delle presenti clausole e del regolamento (UE) 2016/679 e/o del regolamento (UE) 2018/1725.

c) Su richiesta del titolare del trattamento, il responsabile del trattamento gli fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il responsabile del trattamento può espungere informazioni dal contratto prima di trasmetterne una copia.

d) Il responsabile del trattamento rimane pienamente responsabile nei confronti del titolare del trattamento dell'adempimento degli obblighi del sub-responsabile del trattamento derivanti dal contratto che questi ha stipulato con il responsabile del trattamento. Il responsabile del trattamento notifica al titolare del trattamento qualunque inadempimento, da parte del sub-responsabile del trattamento, degli obblighi contrattuali.

e) Il responsabile del trattamento concorda con il sub-responsabile del trattamento una clausola del terzo beneficiario secondo la quale, qualora il responsabile del trattamento sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, il titolare del trattamento ha diritto di risolvere il contratto con il sub-responsabile del trattamento e di imporre a quest'ultimo di cancellare o restituire i dati personali.

7.8. **Trasferimenti internazionali**

a) Qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del responsabile del trattamento è effettuato soltanto su istruzione documentata del titolare del trattamento o per adempiere a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento, e nel rispetto del capo V del regolamento (UE) 2016/679 o del regolamento (UE) 2018/1725.

b) Il titolare del trattamento conviene che, qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento conformemente alla clausola 7.7 per l'esecuzione di specifiche attività di trattamento (per conto del titolare del trattamento) e tali attività di trattamento comportino il trasferimento di dati personali ai sensi del capo V del regolamento (UE) 2016/679, il responsabile del trattamento e il sub-responsabile del trattamento possono garantire il rispetto del capo V del regolamento (UE) 2016/679 utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, del regolamento (UE) 2016/679, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte.

*Clausola 8*

***Assistenza al titolare del trattamento***

a) Il responsabile del trattamento notifica prontamente al titolare del trattamento qualunque richiesta ricevuta dall'interessato. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dal titolare del trattamento.

b) Il responsabile del trattamento assiste il titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, tenuto conto della natura del trattamento. Nell'adempiere agli obblighi di cui alle lettere a) e b), il responsabile del trattamento si attiene alle istruzioni del titolare del trattamento.

c) Oltre all'obbligo di assistere il titolare del trattamento in conformità della clausola 8, lettera b), il responsabile del trattamento assiste il titolare del trattamento anche nel garantire il rispetto dei seguenti obblighi, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del responsabile del trattamento:

1. l'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali («valutazione d'impatto sulla protezione dei dati») qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

2. l'obbligo, prima di procedere al trattamento, di consultare la o le autorità di controllo competenti qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;

3. l'obbligo di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il titolare del trattamento qualora il responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;

4. gli obblighi di cui all'articolo 32 regolamento (UE) 2016/679

d) Le parti stabiliscono nell'allegato III le misure tecniche e organizzative adeguate con cui il responsabile del trattamento è tenuto ad assistere il titolare del trattamento nell'applicazione della presente clausola, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

*Clausola 9*

***Notifica di una violazione dei dati personali***

In caso di violazione dei dati personali, il responsabile del trattamento coopera con il titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del regolamento (UE) 2016/679 o degli articoli 34 e 35 del regolamento (UE) 2018/1725, ove applicabile, tenuto conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

9.1. **Violazione riguardante dati trattati dal titolare del trattamento**

In caso di una violazione dei dati personali trattati dal titolare del trattamento, il responsabile del trattamento assiste il titolare del trattamento:

a) nel notificare la violazione dei dati personali alla o alle autorità di controllo competenti, senza ingiustificato ritardo dopo che il titolare del trattamento ne è venuto a conoscenza, se del caso/(a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);

b) nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del regolamento (UE) 2016/679, devono essere indicate nella notifica del titolare del trattamento e includere almeno:

1. la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

2. e probabili conseguenze della violazione dei dati personali;

3. le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

c) Nell'adempiere, in conformità dell'articolo 34 del regolamento (UE) 2016/679, all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

9.2. **Violazione riguardante dati trattati dal responsabile del trattamento**

In caso di una violazione dei dati personali trattati dal responsabile del trattamento, quest'ultimo ne dà notifica al titolare del trattamento senza ingiustificato ritardo dopo esserne venuto a conoscenza. La notifica contiene almeno:

a) Una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);

b) I recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;

c) Le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

Le parti stabiliscono nell'allegato III tutti gli altri elementi che il responsabile del trattamento è tenuto a fornire quando assiste il titolare del trattamento nell'adempimento degli obblighi che incombono al titolare del trattamento a norma degli articoli 33 e 34 del regolamento (UE) 2016/679.

SEZIONE III

**DISPOSIZIONI FINALI**

*Claudola 10*

**Inosservanza delle clausole e risoluzione**

a) Fatte salve le disposizioni del regolamento (UE) 2016/679 e/o regolamento (UE) 2018/1725, qualora il responsabile del trattamento violi gli obblighi che gli incombono a norma delle presenti clausole, il titolare del trattamento può dare istruzione al responsabile del trattamento di sospendere il trattamento dei dati personali fino a quando quest’ultimo non rispetti le presenti clausole o non sia risolto il contratto. Il responsabile del trattamento informa prontamente il titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole.

b) Il titolare del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali conformemente alle presenti clausole qualora:

1. il trattamento dei dati personali da parte del responsabile del trattamento sia stato sospeso dal titolare del trattamento in conformità della lettera a) e il rispetto delle presenti clausole non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;

2. il responsabile del trattamento violi in modo sostanziale o persistente le presenti clausole o gli obblighi che gli incombono a norma del regolamento (UE) 2016/679 e/o del regolamento (UE) 2018/1725;

3. il responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o della o delle autorità di controllo competenti per quanto riguarda i suoi obblighi in conformità delle presenti clausole o del regolamento (UE) 2016/679 e/o del regolamento (UE) 2018/1725.

c) Il responsabile del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti clausole qualora, dopo aver informato il titolare del trattamento che le sue istruzioni violano i requisiti giuridici applicabili in conformità della clausola 7.1, lettera b), il titolare del trattamento insista sul rispetto delle istruzioni.

d) Dopo la risoluzione del contratto il responsabile del trattamento, a scelta del titolare del trattamento, cancella tutti i dati personali trattati per conto del titolare del trattamento e certifica a quest'ultimo di averlo fatto, oppure restituisce al titolare del trattamento tutti i dati personali e cancella le copie esistenti, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali. Finché i dati non sono cancellati o restituiti, il responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.

*ALLEGATO I*

**Elenco delle Parti**

**Titolare/i del trattamento dati*:*** *[Identità e dati di contatto del/dei titolari del trattamento e, ove applicabile, del suo/loro responsabile della protezione dei dati]*

Nome: Clicca qui per inserire il testo

Indirizzo: Clicca qui per inserire il testo

Nome, qualifica e dati di contatto del referente: Clicca qui per inserire il testo

Firma: Clicca qui per inserire il testo

Data di adesione: Clicca per selezionare la data

\* \* \* \*

**Responsabile/i:** [*Identità e dati di contatto del/dei responsabili del trattamento e, ove applicabile , del suo/loro responsabile della protezione dei dati]*

Nome: Clicca qui per inserire il testo

Indirizzo Clicca qui per inserire il testo

Nome, qualifica e dati di contatto del referente: Clicca qui per inserire il testo

Firma: Clicca qui per inserire il testo

Data di adesione: Clicca per selezionare la data

\* \* \*

*ALLEGATO II*

**Descrizione del trattamento**

*Categorie di soggetti i cui dati personali sono trattati:*

Candidati

Consumatori

Rappresentanti delle concessionarie

Dipendenti

Familiari dei dipendenti

Ex dipendenti

Ospiti

Giornalisti

Membri degli organi sociali

Delegati

Rappresentanti dei fornitori (es. Consulenti, appaltatori, agenti)

Visitatori

*Categorie dei dati personali trattati*

Informazioni identificative: si prega di specificare:

Informazioni di contatto: si prega di specificare:

Informazioni sulla famiglia: si prega di specificare:

Informazioni professionali: si prega di specificare:

Informazioni finanziarie: si prega di specificare:

Informazioni digitali: si prega di specificare:

Informazioni sensibili: si prega di specificare: (qualora possibile)

Altre informazioni: si prega di specificare:

*Dati sensibili trattati (se applicabile) e le restrizioni o garanzie applicate che tengono conto della natura dei dati e dei rischi connessi, come ad esempio una rigorosa limitazione delle finalità, limitazioni all’accesso (tra cui accesso solo per il personale che ha seguito una formazione specifica), tenuta di un registro degli accessi ai dati, limitazione ai trasferimenti successivi o misure di sicurezza aggiuntive.*

*Natura del trattamento*

La prestazione dei servizi ai sensi dell’accordo.

*Finalità per le quali i dati personali sono trattati per conto del titolare del trattamento*

*Durata del trattamento*

Fino al termine del servizio, ad eccezione che vi sia diversa indicazione scritta da parte di Pirelli.

*Per il trattamento dei dati da parte di (sub-) responsabili del trattamento, è necessario specificare anche la materia, la natura e la durata del trattamento.*

La prestazione dei servizi ai sensi del contratto e fino la sua risoluzione, ad eccezione che vi sia diversa indicazione scritta da parte di Pirelli.

*Per i trasferimenti a (sub-) responsabili del trattamento, è necessario descrivere anche le misure tecniche e organizzative che il (sub-) responsabile dovrà adottare per poter fornire assistenza al titolare.*

[*Qualora applicabile*

*ALLEGATO III*

**Misure tecniche e organizzative per garantire la sicurezza dei dati**

Di seguito sono riportate le misure tecniche e organizzative di base che Pirelli richiede ai fornitori che agiscono in qualità di responsabili del trattamento ("**Fornitore/i**") di adottare e implementare per garantire un adeguato livello di sicurezza dei propri dati personali ("**Dati personali Pirelli**"). L'elenco che segue deve essere letto congiuntamente a qualsiasi altro documento tecnico, checklist o certificazione in essere tra Pirelli e il Fornitore sulle misure tecniche e organizzative applicabili al trattamento dei Dati Personali Pirelli.

Nel caso in cui si rendano necessarie modifiche alle misure tecniche e organizzative di base elencate di seguito, il Fornitore dovrà comunicare tempestivamente per iscritto a Pirelli tali modifiche. Tutte le modifiche devono rimanere coerenti con le misure di sicurezza di base generali riportate di seguito e non devono mai portare ad un deterioramento di tali misure.

## **Politiche e procedure**

Il Fornitore dovrà disporre di politiche e/o procedure relative alle aree elencate di seguito. Tali politiche e/o procedure saranno soggette a revisione periodica.

### **Responsabilità**

Il Fornitore dovrà identificare e comunicare a Pirelli i seguenti dettagli: il "*Punto di Contatto*" responsabile della sicurezza informatica degli asset e dei sistemi utilizzati per il trattamento dei Dati Personali Pirelli. Il Fornitore dovrà inoltre comunicare preventivamente a Pirelli i contatti del personale incaricato della comunicazione delle violazioni dei dati personali. Nella misura massima possibile, il Fornitore dovrà anche garantire la disponibilità continua di tale personale 24 ore su 24, 7 giorni su 7, soprattutto in caso di emergenza.

### **Continuità operativa**

Devono essere posti in essere requisiti di sicurezza per garantire il back-up del sistema e la pianificazione della continuità operativa, in particolare per quanto riguarda gli asset utilizzati per il trattamento dei Dati Personali Pirelli. In tale senso, il Fornitore dovrà mantenere la capacità di ripristinare la disponibilità e l'accesso ai Dati Personali Pirelli in modo tempestivo al fine di evitare qualsiasi interruzione del servizio.

### **Formazione e istruzioni sulla sicurezza**

All’interno della struttura aziendale del Fornitore dovranno essere svolte attività di formazione dedicate al miglioramento della consapevolezza della sicurezza informatica. Il personale del Fornitore riceverà istruzioni dettagliate sulla segretezza e sull'integrità delle proprie credenziali di accesso, nonché sulla diligente custodia e protezione dei dispositivi, degli strumenti e dei sistemi ad essi assegnati – con specifico riferimento a quelli utilizzati per il trattamento dei Dati Personali Pirelli.

### **Registrazione e monitoraggio**

I sistemi e gli strumenti utilizzati dal Fornitore per il trattamento dei Dati Personali Pirelli devono disporre di meccanismi di registrazione e monitoraggio. Per quanto riguarda i log, il Fornitore dovrà generare e conservare i log per il periodo previsto dalle leggi applicabili (o altrimenti concordato con Pirelli) e, in ogni caso, conservare tali log per almeno 6 (sei) mesi dalla loro generazione. Per quanto riguarda il monitoraggio, il Fornitore assicurerà la tracciabilità di tutte le operazioni effettuate sui Dati Personali Pirelli attraverso i propri sistemi e strumenti adottando e implementando adeguate misure di tracciamento.

### **Prevenzione della perdita di dati**

Il Fornitore dovrà disporre di politiche e/o procedure che impediscano l'esportazione dei dati al di fuori della rete del Fornitore. In caso di condivisione dei Dati Personali Pirelli, il Fornitore adotterà adeguate misure di riservatezza.

### **Gestione delle violazioni dei dati personali**

Il Fornitore dovrà disporre di politiche e/o procedure relative alla gestione delle violazioni dei dati personali. Tali politiche e procedure dovranno essere conosciute dal personale del Fornitore e periodicamente riviste e verificate dal Fornitore.

## **Gestione degli asset**

### **Inventario degli asset**

Il Fornitore dovrà disporre e mantenere aggiornato un inventario di tutti gli asset utilizzati per il trattamento dei Dati Personali Pirelli.

### **Protezione degli asset**

Il Fornitore dovrà proteggere gli asset utilizzati per il trattamento dei Dati Personali Pirelli secondo gli standard internazionali di settore e le best practice. Le misure di protezione comprendono almeno: l'utilizzo di software antivirus, firewall, moduli IDS/IPS e soluzioni anti-spam.

### **Gestione del ciclo di vita degli asset**

Il Fornitore deve garantire tutti gli asset che trattano i Dati Personali Pirelli, nonché qualsiasi soluzione di cybersecurity richiesta per l'erogazione dei servizi Pirelli (es. antivirus, firewall, moduli IDS/IPS) siano sempre aggiornati all'ultima versione del software disponibile. Nel caso in cui gli aggiornamenti non siano possibili o non ancora applicati, il Fornitore dovrà definire un piano di aggiornamento e un piano complessivo di mitigazione del rischio per gestire qualsiasi rischio rilevante rilevante per l'obsolescenza del sistema (ad es. implementazione della segregazione, monitoraggio, ecc.).

### **Valutazione dei rischi per la sicurezza informatica**

Il Fornitore effettuerà una valutazione dei rischi sui sistemi informatici utilizzati per svolgere i servizi per Pirelli, tenendo conto in particolare di tutti i rischi presentati dal trattamento dei Dati Personali Pirelli. Tale valutazione del rischio dovrà essere effettuata su base annuale o quando richiesto dalle leggi e dai regolamenti applicabili.

## **Crittografia**

### **Misure di crittografia**

Tenendo conto dello stato dell'arte della tecnologia e delle tecniche di crittografia, il Fornitore implementerà la crittografia a diversi livelli:

* **Crittografia a riposo**: il Fornitore adotterà tecniche di cifratura adeguate a proteggere la riservatezza dei Dati Personali Pirelli a riposo a diversi livelli (ad es. crittografia completa del disco su unità di massa; crittografia trasparente dei dati sui database; crittografia a livello di file).
* **Crittografia in transito**: il Fornitore dovrà disporre di adeguate tecniche di crittografia per proteggere la riservatezza dei Dati Personali Pirelli in transito (es. crittografia della rete, crittografia delle applicazioni, ecc.).
* **Gestione delle chiavi di crittografia**: il Fornitore dovrà disporre di soluzioni adeguate e di un processo definito di gestione delle chiavi di crittografia, garantendo almeno la segregazione delle proprietà tra proprietari delle chiavi e proprietari dei dati.
* **Gestione dei certificati di crittografia**: il Fornitore dovrà disporre di soluzioni adeguate e di un processo chiaro e documentato per la gestione dei certificati di crittografia. Tale processo dovrà essere sviluppato in base ai requisiti definiti dagli standard industriali internazionali (ad esempio, lunghezza minima delle chiavi di crittografia).

## **Gestione delle identità e degli accessi**

### **Accesso ai Dati Personali Pirelli**

Il Fornitore garantisce che l’accesso ai Dati Personali Pirelli potrà essere consentito solo a personale autorizzato con adeguate competenze ed esperienze in materia di protezione dei dati e che tale personale sarà soggetto a obblighi di riservatezza.

Il Fornitore dovrà tenere e aggiornare regolarmente un elenco di tutte le persone (inclusi i dipendenti, gli agenti o gli appaltatori) che agiscono sotto la sua autorità o sotto l'autorità di eventuali sub-responsabili del trattamento, che hanno accesso ai Dati Personali Pirelli o che li trattano in altro modo.

### **Misure e principi per l'identificazione e l'autorizzazione dell'utente**

Il Fornitore dovrà implementare sistemi per l'autenticazione degli utenti e la gestione delle autorizzazioni. Il Fornitore assegnerà i permessi minimi di accesso ai Dati Personali Pirelli secondo i principi di “Least *privilege and Need-to-know*" (ossia consentendo l'accesso solo ai dati necessari per svolgere la relativa funzione lavorativa). Il Fornitore dovrà inoltre rivedere le autorizzazioni da concedere agli utenti sulla base del loro ruolo nel trattamento dei Dati Personali Pirelli, nonché alla luce di eventuali requisiti normativi applicabili in materia di gestione delle identità e degli accessi degli utenti.

### **Revisione del profilo**

Il Fornitore dovrà verificare la coerenza e la presenza dei profili di autorizzazione degli utenti con cadenza almeno annuale e terrà traccia di tale attività quando si tratta di Dati Personali Pirelli.

### **Sicurezza** **delle credenziali**

Il Fornitore adotterà standard internazionali e best practice sui requisiti di sicurezza delle credenziali su tutti gli asset utilizzati per il trattamento dei Dati Personali Pirelli.

### **Credenziali individuali**

Il Fornitore dovrà assegnare solo credenziali individuali su tutti gli asset utilizzati per il trattamento dei Dati Personali Pirelli (in particolare quelli con autorizzazioni elevate su sistemi e applicazioni). È severamente vietata l’assegnazione e l’utilizzo di credenziali condivise.

### **Ciclo di vita delle identità**

Il fornitore deve disporre di un processo chiaro per la gestione del ciclo di vita dell'identità. Tale processo deve garantire che tutte le credenziali utilizzate per accedere agli asset utilizzati per il trattamento dei Dati Personali Pirelli scadano automaticamente dopo un periodo predeterminato di mancato utilizzo da parte degli utenti.

# **Sicurezza fisica**

### **Sicurezza dei centri di elaborazione dati ("DPC")**

Il Fornitore dovrà disporre di misure di sicurezza fisica sviluppate secondo i principali standard di settore e le best practice quali, almeno: installazione di sistemi di allarme antifurto e telecamere a circuito chiuso, sia per quanto riguarda i locali che gli ingressi ai DPC. Il Fornitore dovrà inoltre disporre di procedure per limitare l'accesso fisico ai DPC (es. tornelli antintrusione), prevenire attività non autorizzate e segnalare attività di accesso (es. tentativi multipli di accesso non riusciti).

### **Posizionamento dei DPC**

Il Fornitore comunicherà a Pirelli, su richiesta, l'ubicazione dei DPC utilizzati per il trattamento dei Dati Personali Pirelli. Pirelli deve essere informata preventivamente in caso di eventuali variazioni all’ubicazione dei DPC.

# **Operazioni di sicurezza**

### **Sicurezza del sistema**

Il Fornitore dovrà adottare misure adeguate a ridurre le vulnerabilità degli asset utilizzati per il trattamento dei Dati Personali Pirelli, applicando configurazioni adeguate ed evitando modifiche non autorizzate (ad esempio, il controllo del dispositivo rimovibile).

### **Linee guida per lo sviluppo della sicurezza**

In caso di sviluppo del software utilizzato per il trattamento dei Dati Personali Pirelli, il Fornitore dovrà adottare linee guida per la scrittura di codice sicuro.

### **Gestione delle patch di sicurezza**

Il Fornitore dovrà gestire l'installazione e la disinstallazione delle patch con un processo, sviluppato secondo le best practice e gli standard del settore, che garantisca la tracciabilità e la tempistica delle attività di patching.

### **Valutazione della** **vulnerabilità**

Il Fornitore dovrà fornire evidenza delle attività di valutazione delle vulnerabilità o delle attività di penetration test eseguite sui propri sistemi.

# **Violazioni dei dati personali**

### **Notifica a Pirelli**

In caso di violazione dei dati personali relativi ai Dati personali Pirelli, il Fornitore dovrà darne tempestiva comunicazione a Pirelli tramite [Personal\_Data\_Breach@pirelli.com](mailto:Personal_Data_Breach@pirelli.com). I termini per la notifica della violazione sono i seguenti:

1. **Informazioni chiave** (semplice comunicazione via e-mail comprendente almeno gli elementi descritti nelle clausole pertinenti delle SCC): entro e non oltre 12 ore dal momento in cui si è venuti a conoscenza della violazione.
2. **Report completo** (basato sul Security *Incident Report* disponibile a questo [link](https://psi-dotcom-prd.s3.eu-west-1.amazonaws.com/suppliers-portal/it-it/Security_Incident_Report_IT.docx) o, in alternativa, su un formato dedicato del Fornitore, che includa le informazioni richieste nel Security Incident Report Pirelli): entro e non oltre 48 ore dalla notifica delle informazioni chiave di cui sopra

*Allegato IV*

**Lista dei sub responsabili**

Il titolare ha autorizzato il ricorso ai seguenti sub responsabili:

Nome: Clicca per inserire il testo

Indirizzo: Clicca per inserire il testo

Nome, qualifica e dati di contatto del referente: Clicca per inserire il testo

Descrizione del trattamento (includendo una chiara delimitazione delle responsabilità qualora vengano incaricati più sub responsabili): Clicca per inserire il testo

\* \* \* \*