

CONTRATTO PER IL TRATTAMENTO DEI DATI PERSONALI CON IL RESPONSABILE

ai sensi dell'art. 28, paragrafo 7, del Regolamento (UE) 2016/679.

Il presente Contratto definisce le modalità con le quali il Responsabile del trattamento si impegna ad effettuare per conto del Titolare le operazioni di trattamento dei dati personali.

Per la redazione dello Stesso sono state utilizzate le Clausole Contrattuali Tipo (anche dette "SCC") tra titolari del trattamento e responsabili del trattamento, adottate a norma dell'articolo 28, paragrafo 7, del Regolamento (UE) 2016/679 (in seguito anche "GDPR") con la **Decisione di esecuzione (UE) 2021/915 della Commissione del 4 giugno 2021 (Testo rilevante ai fini del SEE)**.

Tale Contratto, **firmato dalle Parti negli appositi spazi dell'Allegato I, è accluso al contratto di**
..... della ditta stipulato in data
....., tra:

Titolare del trattamento:

FONDAZIONE IRCCS SAN GERARDO DEI TINTORI

Via G. B. Pergolesi n. 33

20900 Monza (MB)

Nome, qualifica e dati di contatto:

Dr. Silvano Casazza - in qualità di Direttore Generale

PEC: protocollo@pec.irccs-sangerardo.it

Responsabile/i del trattamento:

[Fornitore]

Via

Nome, qualifica e dati di contatto del referente:

Dr. , in qualità di Legale Rappresentante di

Con la sottoscrizione del presente Contratto il Responsabile del trattamento, attenendosi alle istruzioni impartite dal Titolare nel pieno rispetto di quanto imposto dall'art. 28, par. 3, del GDPR si impegna a mettere in atto misure tecniche e organizzative adeguate che rispettino il GDPR e la sicurezza del trattamento, garantendo la tutela dei diritti degli interessati.

Si premette altresì che:

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 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, nonché 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 o 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

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 30 giorni, 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.

- a) 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.
- b) 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.
- c) 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.

- d) 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) le 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 entro 36 ore dalla conoscenza del fatto. 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

Clausola 10

Inosservanza delle clausole e risoluzione

- a) Fatte salve le disposizioni del regolamento (UE) 2016/679 e/o del 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: [Identità e dati di contatto del/dei titolari del trattamento e, ove applicabile, del suo/loro responsabile della protezione dei dati]

Nome: FONDAZIONE IRCCS SAN GERARDO DEI TINTORI

Indirizzo: Via G. B. Pergolesi n. 33 – 20900 Monza (MB)

Nome, qualifica e dati di contatto del titolare: Dr. Silvano Casazza - Direttore Generale - PEC protocollo@pec.irccs-sangerardo.it

Firma e data di adesione:

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

Nome: [Fornitore].....

Indirizzo:

Nome, qualifica e dati di contatto del referente:

Firma e data di adesione:

Punti di contatto del titolare e del responsabile del trattamento

1. Le parti possono mettersi in contatto tra di loro utilizzando i seguenti punti di contatto:
2. Le parti sono tenute a informarsi costantemente di ogni modifica riguardante i punti di contatto.

Titolare del trattamento

DPO	Nome e Cognome: Ing. MAURIZIO PASTORE - LIGURIA DIGITALE S.p.A. di Genova Email: privacyweb@liguriadigitale.it pec: protocollo@pec.liguriadigitale.it Contatto telefonico: 010/6545441 - 335/1302371
DIREZIONE AMMINISTRATIVA	Email e/o pec: protocollo@pec.irccs-sangerardo.it Contatto telefonico: 039/2339702
Ufficio/Referente Privacy	Nome e Cognome: MARIAGRAZIA MERONI Email e/o pec: mariagrazia.meroni@irccs-sangerardo.it Contatto telefonico: 039/2339705
Rappresentante UE del Titolare del trattamento	Nome e Cognome: Email e/o pec: Contatto telefonico:
CISO	Nome e Cognome: dott. DAVIDE TOME' Email e/o pec: davide.tome@irccs-sangerardo.it Contatto telefonico: 039/2339009 – 335/5733153
Referente tecnico (ad es: Direttore dell'esecuzione, Amministratore di Sistema, Ing.	Nome e Cognome: Email e/o pec:

Clinico)	Contatto telefonico:
Referente Unico del Procedimento (RUP)	Nome e Cognome: Email e/o pec: Contatto telefonico:
Direttore Esecuzione Contratto (DEC)	Nome e Cognome: Email e/o pec: Contatto telefonico:

Responsabile del trattamento

DPO	Nome e Cognome: Email e/o pec: Contatto telefonico:
Segreteria Generale	Nome e Cognome: Email e/o pec: Contatto telefonico:
Referente dell'Ufficio Privacy	Nome e Cognome: Email e/o pec: Contatto telefonico:
Rappresentante UE del Responsabile del trattamento	Nome e Cognome: Email e/o pec: Contatto telefonico:
CISO	Nome e Cognome: Email e/o pec: Contatto telefonico:
Referente tecnico (ad es: Amministratore di Sistema, Ing. Clinico)	Nome e Cognome: Email e/o pec: Contatto telefonico:
Responsabile Unico delle Attività Contrattuali (RUAC)	Nome e Cognome: Email e/o pec: Contatto telefonico:
Direttore Esecuzione Contratto (DEC)	Nome e Cognome: Email e/o pec: Contatto telefonico:

ALLEGATO II

Descrizione del trattamento

Categorie di interessati i cui dati personali sono trattati

- ☐ a) Dipendenti/Consulenti
- ☐ b) Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)
- ☐ c) Associati, soci, aderenti, simpatizzanti, sostenitori
- ☐ d) Soggetti che ricoprono cariche sociali
- ☐ e) Beneficiari o assistiti
- ☐ f) Pazienti
- ☐ g) Minori
- ☐ h) Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
- ☐ i) Altro [.....]

Categorie di dati personali trattati

- ☐ a) Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale)
- ☐ b) Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
- ☐ c) Dati di accesso e di identificazione (username, password, customer ID, altro...)
- ☐ d) Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro...)
- ☐ e) Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione Internet, altro...)
- ☐ f) Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza
- ☐ g) Dati di profilazione
- ☐ h) Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro...)
- ☐ i) Dati relativi all'ubicazione
- ☐ l) Dati che rivelano l'origine razziale o etnica
- ☐ m) Dati che rivelano le opinioni politiche
- ☐ n) Dati che rivelano le convinzioni religiose o filosofiche
- ☐ o) Dati che rivelano l'appartenenza sindacale
- ☐ p) Dati relativi alla vita sessuale o all'orientamento sessuale
- ☐ q) Dati relativi alla salute
- ☐ r) Dati genetici
- ☐ s) Dati biometrici
- ☐ t) Altro [.....]

Commentato [1]: AD ESEMPIO:

- cittadini,
- disabili,
- referenti aziende clienti;
- rappresentanti legali aziende potenziali;
- personale dipendente delle aziende clienti;
- etc etc da individuare]

Commentato [2]: [di seguito alcuni esempi: eliminare e/o aggiungere in base ai dati personali effettivamente trattati]
Dati comuni:

- caratteristiche individuali (ad es. peso, altezza ecc.),
- codice fiscale e altri codici identificativi (matricola lavoratore);
- indirizzo di residenza e/o domicilio,
- n. carta d'identità,
- indirizzo IP,
- codice IBAN,
- n. di targa,
- dati personali contenuti nel cedolino dello stipendio;
- dati reddituali e compensi percepiti;
- informazioni presenti nel curriculum vitae;
- Informazioni aventi natura "soggettiva" quali opinioni o valutazioni, anche espresse con codici o in termini numerici (valutazioni della prestazione/capacità lavorativa/l'affidabilità; notizie contenute nelle relazioni/consulenze/perizie; esito di test psicologici/disegni; informazioni contenute sotto forma di testo libero come un messaggio di posta elettronica; risposte scritte fornite da un candidato durante un esame professionale e le eventuali annotazioni dell'esaminatore relative a tali risposte; etc.....)

Dati sensibili trattati (se del caso) e limitazioni o garanzie applicate che tengono pienamente conto della natura dei dati e dei rischi connessi, ad esempio una rigorosa limitazione delle finalità, limitazioni all'accesso (tra cui accesso solo per il personale che ha seguito una formazione specializzata), tenuta di un registro degli accessi ai dati, limitazioni ai trasferimenti successivi o misure di sicurezza supplementari.

Con riferimento alle categorie particolari di dati (cd. sensibili), in ossequio al Provvedimento del Garante Privacy n. 146 del 5 giugno 2019 (Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 176 del 29 luglio 2019), il Responsabile del trattamento adotterà - in ogni caso - per il trattamento di:

- ☐ categorie particolari di dati nei rapporti di lavoro, le Prescrizioni di cui all'aut. gen. n. 1/2016;
- ☐ categorie particolari di dati da parte degli organismi di tipo associativo, delle fondazioni, delle chiese e associazioni o comunità religiose, le Prescrizioni di cui all'aut. gen. n. 3/2016;
- ☐ categorie particolari di dati da parte degli investigatori privati, le Prescrizioni di cui all'aut. gen. n. 6/2016;
- ☐ dati genetici e i campioni biologici, le Prescrizioni di cui all'aut. gen. n. 8/2016;
- ☐ dati personali per scopi di ricerca scientifica, le Prescrizioni di cui all'aut. gen. n. 9/2016;
- ☐ nessuna delle Prescrizioni di cui *supra*.

Il Responsabile deve essere in grado di dimostrare, laddove necessario, il rispetto delle succitate specifiche prescrizioni.

Natura del trattamento

Il trattamento potrà essere svolto in **maniera manuale, informatizzata e con l'intervento umano**

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

Resta inteso che se il Responsabile del trattamento viola il Regolamento (UE) 2016/679, ovvero agisce in modo difforme o contrario rispetto alle legittime istruzioni impartite dal Titolare, determinando le finalità e i mezzi del trattamento, è da considerarsi quale Titolare del trattamento in questione (cfr. art. 28, paragrafo 10, del GDPR).

Durata del trattamento

Il trattamento potrà essere svolto fino al termine della durata contrattuale ovvero fino al **XXXXXXXXXX**; se anteriore, fino alla cessazione di efficacia del contratto.

Al termine o alla cessazione di efficacia del contratto il Responsabile del trattamento deve restituire al Titolare tutti i dati personali trattati per suo conto e cancellare le eventuali copie esistenti in suo possesso (su qualsiasi supporto) secondo le istruzioni ricevute dal Titolare, certificando altresì a quest'ultimo di averlo fatto, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali.

Il Titolare può effettuare tale verifica tramite un revisore, anche di terza parte, a condizione che non abbia una relazione competitiva con il Responsabile stesso.

Inoltre, è esplicitamente esclusa la pratica del "blocco da fornitore" (c.d. Vendor lock-in).

Finché i dati non sono restituiti e cancellati, il Responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.

Per il trattamento da parte di (sub-)responsabili del trattamento, specificare anche la materia disciplinata, la natura e la durata del trattamento.

Commentato [3]: Dati sensibili/particolari:

- origine razziale o etnica
- opinioni politiche
- convinzioni religiose o filosofiche
- appartenenza sindacale
- dati genetici
- dati biometrici (immagini registrate da un sistema di videosorveglianza);
- dati relativi alla salute: idoneità al lavoro [compreso informazioni di cui è vietata in ogni caso la pubblicazione a "erogazione ai sensi della legge 104/1992"; "soggetto portatore di handicap"; "anziano non autosufficiente"; "indici di autosufficienza nelle attività della vita quotidiana"; "contributo per ricovero in struttura sanitaria" o per "assistenza sanitaria"]
- dati relativi alla vita sessuale o all'orientamento sessuale;
- Dati giudiziari:
- informazioni relative a condanne penali e a reati, o a connesse misure di sicurezza.

Commentato [4]: L'utilizzo di intelligenza artificiale e algoritmi - da evitare - è da indicare puntualmente: richiede generalmente una DPIA ovvero una valutazione d'impatto. PS: nel caso contattare il DPO

ALLEGATO III

Misure tecniche e organizzative, comprese misure tecniche e organizzative per garantire la sicurezza dei dati

NOTA ESPLICATIVA:

Le misure tecniche e organizzative devono essere descritte in modo concreto e non genericamente.

Descrizione delle misure di sicurezza tecniche e organizzative messe in atto dal o dai Responsabili del trattamento (comprese le eventuali certificazioni pertinenti) per garantire un adeguato livello di sicurezza, tenuto conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche.

1) PRIVACY BY DESIGN E BY DEFAULT:

Il Responsabile del trattamento deve rispettare i principi di protezione dei dati fin dalla progettazione (*privacy by design*) e protezione dei dati per impostazione predefinita (*privacy by default*) di cui all'art. 25 GDPR comunicando al Titolare le soluzioni individuate ed adottate per rispettare tali principi (cfr. Considerando 78 GDPR).

2) ELENCO AGGIORNATO SUB-RESPONSABILI:

Quando il primo responsabile del trattamento è autorizzato a ricorrere a un altro responsabile del trattamento per l'esecuzione di specifiche attività, a prescindere dal carattere specifico o generale dell'autorizzazione preliminare scritta del Titolare del trattamento, il primo responsabile deve tenere un elenco aggiornato degli altri (sub-)responsabili (sulla scorta dell'Allegato IV). Su richiesta del titolare e/o in caso di accertamenti anche da parte del Garante, il primo responsabile del trattamento gli fornisce prontamente e non oltre 24 ore copia dell'elenco aggiornato.

3) ATTIVITA' DI REVISIONE, COMPRESSE LE ISPEZIONI:

Su richiesta del titolare del trattamento, a intervalli annuali o se vi sono indicazioni di inosservanza, il responsabile del trattamento consentirà e contribuirà alle attività di revisione delle attività di trattamento di cui alle presenti clausole. Nel decidere in merito a un riesame o a un'attività di revisione, il titolare del trattamento potrà tenere conto delle pertinenti certificazioni in possesso del responsabile del trattamento.

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 di almeno 72 ore.

4) TRASFERIMENTO DATI EXTRA UE:

È vietato qualunque trasferimento di dati da parte del responsabile del trattamento verso un paese terzo o un'organizzazione internazionale, ovvero a sub-responsabili del trattamento che non rientrano nell'ambito di applicazione territoriale del GDPR, compresi trasferimenti successivi.

Il responsabile del trattamento si assicura che anche il sub-responsabile del trattamento non effettui trasferimenti di dati verso un paese terzo o un'organizzazione internazionale.

In presenza di una decisione di adeguatezza (cfr. <https://www.garanteprivacy.it/temi/trasferimento-di-dati-all-estero>), il Responsabile del trattamento è tenuto in ogni caso a chiedere specifica autorizzazione al Titolare, in considerazione degli obblighi connessi ai trasferimenti internazionali di cui al capo V del GDPR.

In generale, il trasferimento di dati extra UE può essere 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 GDPR.

5) AMMINISTRATORE DI SISTEMA:

Nel caso in cui il Responsabile effettua trattamenti, anche in parte, mediante strumenti elettronici, si impegna ad individuare e a designare gli Amministratori di Sistema ("AdS"), conformandosi altresì, nell'affidamento di tale incarico, a tutto quanto previsto dal provvedimento del Garante Privacy del 27 novembre 2008 [doc. web n. 1577499] (G.U. n. 300 del 24 dicembre 2008), come modificato in base al provvedimento del 25 giugno 2009.

Le persone fisiche designate AdS considerate come tali sono le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti nonché altre figure equiparabili quali gli amministratori di base dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Delle misure e degli accorgimenti prescritti con la designazione di Amministratore di Sistema il Responsabile del trattamento è tenuto a darne la prova; deve altresì conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali Amministratori di Sistema, tenendo costantemente aggiornato tale documento interno (come da Allegato V) e in caso di accertamenti anche da parte del Garante fornire prontamente e comunque entro 24 ore il medesimo documento al Titolare.

6) MISURE MINIME E MISURE AGID:

Il Responsabile deve dotarsi delle misure minime di sicurezza per limitare il rischio di attacchi informatici.

Per il tramite degli Amministratori di Sistema designati, si impegna a garantire di *default* le modalità tecniche previste dall'Allegato B del Codice Privacy (*Disciplinare tecnico in materia di misure di sicurezza*), seppur oggi abrogato.

Il Responsabile si impegna ad installare e mantenere aggiornate, sugli strumenti elettronici oggetto del contratto, tutte le misure e gli accorgimenti eventualmente prescritti dai Provvedimenti emessi dall'Autorità Garante per la protezione dei dati personali (GPDP), dall'Agenzia per l'Italia Digitale (AGID) e dall'Agenzia per la Cybersicurezza Nazionale (ACN), applicabili al servizio commissionato, nonché le ulteriori misure di sicurezza previste nel contratto di fornitura.

Nello specifico, il Responsabile si impegna al rispetto e alla dimostrazione di quanto previsto dall'AGID con:

- le Linee guida - Sicurezza nel Procurement ICT (Pubblicato il 19/05/2020 - Aggiornato il 19/05/2020) e disponibile anche alla

Commentato [5]: per i trattamenti di dati sensibili svolti dai soggetti pubblici (quelli di cui all'art. 6.1.c) ed e) del GDPR), in considerazione dell'art. 6.2 del GDPR saranno valutate le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 del Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

Commentato [GDPR CC6]: Misure necessarie per le PP.AA., valide quale riferimento pratico per valutare e migliorare il livello di sicurezza informatica e contrastare le minacce informatiche più frequenti.

seguente

url:

https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/2013910214200_OLG_Sicurezza_Procurement_ICT_versione_finale_pub.pdf

- Linee guida per lo sviluppo del software sicuro (Ultimo aggiornamento 06-05-2020), disponibile alla seguente url: <https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro>

- le «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)». (17A03060) (GU Serie Generale n.103 del 05-05-2017), disponibili anche alla seguente url: <https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict>

7) MISURE ULTERIORI:

Inoltre il Responsabile del trattamento si impegna a mettere in atto misure tecniche e organizzative più specifiche, ferma la dimostrazione della loro adozione, quali:

a) mezzi che permettono di garantire la confidenzialità, l'integrità, la disponibilità e la resilienza costante dei sistemi e dei servizi di trattamento.

a.1) la capacità di assicurare la riservatezza dei dati trattati, facendo in modo che le password relative alle utenze dei soggetti autorizzati siano di lunghezza non inferiore a otto caratteri e siano sottoposte a un controllo automatico di qualità che impedisca l'uso di password "deboli" e che le medesime password siano modificate almeno al primo utilizzo;

a.2) la capacità di assicurare la riservatezza dei dati trattati, facendo in modo che l'autenticazione dei soggetti autorizzati avvenga tramite un processo di autenticazione multifattoriale (MFA);

a.3) la capacità di contrastare efficacemente attacchi informatici di tipo brute force sul sistema di autenticazione online, anche introducendo limitazioni al numero di tentativi infruttuosi di autenticazione;

a.4) crittografia dei dati che i dispositivi del fornitore/responsabile (computer, portatili, tablet, ecc.) devono rispettare;

a.5) l'accesso alla rete locale dell'amministrazione da parte del fornitore/responsabile deve essere configurato con le abilitazioni strettamente necessarie alla realizzazione di quanto contrattualizzato, vale a dire consentendo l'accesso esclusivamente alle risorse necessarie. L'accesso dall'esterno mediante VPN deve essere consentito, solo se strettamente necessario, utilizzando account VPN personali configurati e abilitati opportunamente. Gli accessi dovranno poter essere tracciati per eventuali successivi audit;

a.6) nelle forniture di sviluppo e manutenzione, l'utilizzo dei dati dell'amministrazione per la realizzazione di quanto contrattualizzato deve essere consentito esclusivamente su server/database di sviluppo nei quali sono stati importati i dati necessari per gli scopi del progetto. Pertanto, questa misura consiste nel gestire l'accesso ai server e ai DB in modo da rispettare questa regola generale, tracciando le eventuali eccezioni che dovessero verificarsi;

b) mezzi che permettono di ristabilire la disponibilità dei dati a carattere personale e l'accesso a questi nei tempi appropriati in caso di incidente fisico o tecnico;

c) rilevare e detenere a norma di legge copia dei log di accesso all'applicativo e di sistema;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

e) nomina di un DPO, nei casi previsti dall'art. 37 GDPR ovvero per i soggetti privati obbligati alla sua designazione. Nel caso in cui il Responsabile del trattamento ritenesse tale nomina non obbligatoria, alla luce del principio di *accountability* è tenuto a dare la prova della mancanza dei criteri di nomina (cfr. Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato, punto nn. 3 e 4);

f) poter dimostrare che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal Responsabile del trattamento e non abbia ricevuto idonea formazione;

g) una procedura per la gestione degli incidenti di sicurezza e delle violazioni di dati personali (cd. "Data Breach");

h) sottoscrizione di polizze assicurative che tengano conto dei risarcimenti danni di cui all'art. 82 del GDPR con massimali adeguati;

i) il Responsabile è tenuto ad effettuare preliminarmente, e indipendentemente dal titolare del trattamento, una Valutazione del Rischio per la sicurezza dei dati che tenga in considerazione i rischi presentati dal trattamento come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati (cfr. considerando 83 GDPR). E' inteso che nel caso in cui il responsabile;

i) laddove la tipologia del trattamento rientri nell'elenco di cui all'ALLEGATO 1 AL PROVVEDIMENTO N. 467 DELL'11 OTTOBRE 2018 [doc. web n. 9058979] (Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018), il Responsabile è tenuto ad effettuare preliminarmente, e indipendentemente dal titolare del trattamento, una Valutazione d'impatto sul prodotto/servizio;

l) (R12) Sulle reti messe a disposizione dal fornitore devono essere presenti di dispositivi di sicurezza perimetrale con funzioni di sicurezza (ad esempio Firewall e sistemi di Network Detection ed Event & Log Monitoring, SIEM, ecc.) necessari a rilevare e contenere eventuali incidenti di sicurezza ICT e in grado di gestire gli IoC (Indicator of Compromise);

m) (R13) Il fornitore deve usare protocolli cifrati e meccanismi di autenticazione nell'ambito dei servizi erogati;

n) (R14) Qualora il fornitore subisca un attacco, in conseguenza del quale vengano compromessi sistemi del committente da lui

Commentato [GDPR CC7]: Quanto indicato in giallo va adattato alla singola realtà.

Commentato [8]: Cfr. Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato
(3. Chi sono i soggetti privati obbligati alla sua designazione? a titolo esemplificativo e non esaustivo: istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; sindacati; caf e patronati; società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas); imprese di somministrazione di lavoro e ricerca del personale; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione; società di call center; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento.)

gestiti, deve farsi carico delle bonifiche del caso, e riportare i sistemi in uno stato di assenza di vulnerabilità.

o) (R15) Il fornitore si impegna a trattare, trasferire e conservare le eventuali repliche dei dati oggetto di fornitura, ove autorizzate dalle amministrazioni, sempre all'interno del territorio dell'UE.

7.1) Verificare la documentazione finale di progetto

Alla fine di ogni singolo progetto (che come specificato in precedenza non coincide necessariamente col termine del contratto), l'amministrazione deve verificare che il fornitore rilasci la seguente documentazione:

- documentazione finale e completa del progetto;
- manuale di installazione/configurazione;
- report degli Assessment di Sicurezza eseguiti con indicazione delle vulnerabilità riscontrate e le azioni di risoluzione/mitigazione apportate.
- "libretto di manutenzione" del prodotto (software o hardware), con l'indicazione delle attività da eseguire per mantenere un adeguato livello di sicurezza del prodotto realizzato o acquistato. In particolare, nel libretto di manutenzione deve essere indicato:
 - produttore e versione dei prodotti software utilizzati (ad esempio web server, application server, CMS, DBMS), librerie, firmware;
 - indicazioni per il reperimento dei Bollettini di Sicurezza dei singoli produttori di hardware/software;
 - indicazioni sul processo di installazione degli aggiornamenti sicurezza;
 - documento di EoL (documento che contiene indicazione dei prodotti utilizzati e relativo fine vita/rilascio aggiornamenti sicurezza);

7.2) Distruzione del contenuto logico (wiping) dei dispositivi che vengono sostituiti

Nelle acquisizioni di attività di conduzione CED o di gestione di parchi di PC (fleet management), occorre verificare che l'hardware dismesso, si tratti di server o di postazioni di lavoro, venga cancellato e distrutto in modo sicuro, evitando rischi che dati critici possano restare erroneamente memorizzati sull'hardware dismesso.

Anche in questo caso, scrivere il requisito nel capitolato non è sufficiente: va definito un processo di verifica strutturato. Il processo può prevedere:

- la consegna di un verbale di avvenuta distruzione da parte del fornitore,
- nel caso di sistemi critici, un'eventuale azione ispettiva che può ad esempio far parte delle attività di monitoraggio.

7.3) Manutenzione - aggiornamento dei prodotti:

- gli amministratori di sistema devono obbligatoriamente eseguire gli aggiornamenti ogni qualvolta sui siti dei produttori vengono rilasciati patch e correzioni per problemi di vulnerabilità.

7.4) Vulnerability Assessment

Il Fornitore/Responsabile deve eseguire, su beni e servizi classificati critici ed esposti sul web, un Vulnerability Assessment a cadenza almeno annuale, e ogni volta che si apportano modifiche alla configurazione software/hardware.

8) PERSONALE AUTORIZZATO:

Il Responsabile del trattamento si impegna a produrre ed aggiornare in caso di modifiche l'elenco degli operatori autorizzati singolarmente ed opportunamente formati in materia di privacy (ivi inclusi gli opportuni aggiornamenti normativi), impartendo per iscritto specifiche istruzioni per trattare i dati degli utenti nell'ambito della propria attività e con i limiti di legge, curando, in particolare, il profilo della sicurezza e dell'integrità dei dati ai sensi dell'art. 29 del GDPR. Inoltre, il Responsabile s'impegna a stabilire le modalità di accesso ai dati e l'organizzazione del lavoro degli autorizzati al trattamento, avendo cura di adottare preventivamente misure organizzative adeguate al rischio per diritti e libertà delle persone fisiche. Inoltre deve garantire che le persone autorizzate siano state istruite sulla procedura di gestione degli incidenti di sicurezza e la gestione delle violazioni di dati personali. Il Titolare può richiedere una prova documentata al fine di verificare tali adempimenti.

9) REGISTRO DEL TRATTAMENTO:

Il Responsabile del trattamento, anche laddove non rientri nelle casistiche definite dall'art. 30, par. 2 e 5, del GDPR tiene per iscritto un Registro delle attività relative ai trattamenti svolti per conto del Titolare.

10) ASSISTENZA AL TITOLARE:

In generale, il responsabile del trattamento è tenuto ad assistere il titolare nel garantire il rispetto degli obblighi a cui è vincolato quest'ultimo e a rispondere prontamente e comunque non oltre 72 ore dalle richieste di informazioni del titolare del trattamento.

Il Responsabile comunicherà ogni informazione utile al fine di assistere il titolare nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti. Qualora il responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti, informa senza indugio e comunque non oltre 72 ore il titolare affinché possa garantire che i dati personali siano esatti e aggiornati.

Nel caso in cui riceva richieste degli interessati per l'esercizio dei loro diritti, il responsabile notifica prontamente e comunque non oltre 72 ore al titolare del trattamento qualunque richiesta ricevuta dall'interessato in quanto non è autorizzato a rispondere egli stesso alla

richiesta.

Inoltre, il Responsabile del trattamento assiste il Titolare nel garantire il rispetto degli obblighi imposti a quest'ultimo ai sensi dell'articolo 32 del GDPR, fornendogli, tra l'altro, le informazioni riguardanti le misure tecniche e organizzative da questi adottate in conformità all'articolo 32 medesimo, unitamente a tutte le altre informazioni necessarie al Titolare del trattamento per conformarsi agli obblighi a lui imposti per garantire un livello di sicurezza adeguato al rischio.

Il Responsabile si impegna a predisporre, condividere e aggiornare periodicamente la valutazione del rischio per la sicurezza dei dati (v. ad es.: <https://www.enisa.europa.eu/risk-level-tool/risk>) e la valutazione di impatto sulla protezione dei dati cfr. <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/8581268>) e, comunque, a redigere uno o più atti di documentazione delle scelte, dando atto della conformità alla normativa sulla protezione delle persone con riguardo al trattamento dei dati e alla circolazione dei dati, ovvero indicando che il trattamento presenterebbe un rischio elevato.

Laddove la valutazione di impatto sulla protezione dei dati presentasse un rischio elevato, anche in fase di consultazione con la/le autorità di controllo competenti, il responsabile assisterà il titolare del trattamento per adottare le misure adeguate per attenuare il rischio.

Il responsabile si impegna ad adibire apposito ufficio/referente, segnalando un punto di contatto diretto al titolare del trattamento, alle incombenze relative alla notificazione e comunicazioni previste dal GDPR.

11) COMUNICAZIONE E REGISTRO DI INCIDENTI DI SICUREZZA E DI VIOLAZIONI DI DATI PERSONALI:

In caso di incidente di sicurezza e/o di violazione dei dati personali (cd. Data Breach), senza indugio il responsabile del trattamento coopera con il titolare e lo assiste nell'adempimento degli obblighi, ai sensi degli artt. 33 e 34 GDPR.

Nel caso di incidente di sicurezza e/o di una violazione dei dati personali trattati dal responsabile del trattamento, quest'ultimo ne dà comunicazione al titolare senza ingiustificato ritardo e comunque non oltre 24 ore dopo esserne venuto a conoscenza. La comunicazione iniziale contiene le informazioni disponibili in quel momento e le altre informazioni sono fornite non appena disponibili, senza ingiustificato ritardo. Il responsabile documenta qualsiasi incidente di sicurezza e/o di violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Il responsabile deve mantenere un Registro degli incidenti di sicurezza, anche qualora non vi siano delle violazioni dei dati personali, per coadiuvare il Titolare nel suo obbligo relativo al paragrafo 5 dell'art. 33 del GDPR.

A seguito del verificarsi di detti incidenti il Titolare potrà:

- effettuare le succitate attività di revisione, comprese le ispezioni (v. misura n. 3);
- prescrivere l'adozione di misure di sicurezza aggiornate e/o ulteriori anche rispetto a quelle previste dal presente accordo;
- attivare azioni di rivalsa nei confronti del Responsabile;
- applicare le penali contrattuali;
- risolvere il contratto (cfr. la succitata Clausola 10).

Il Responsabile deve adottare procedure tecniche e organizzative volte alla gestione di eventuali incidenti di sicurezza e di violazioni di dati personali; deve disporre altresì di una struttura per la prevenzione e gestione degli incidenti informatici e delle violazioni di dati personali con il compito d'interfacersi con le analoghe strutture del Titolare.

12) LINEE GUIDA E PROVVEDIMENTI DELL'AUTORITA' GARANTE PRIVACY:

Il Responsabile del trattamento s'impegna a mettere in atto le misure tecniche e organizzative previste da Linee Guida e provvedimenti adottati dalle Autorità europee in materia di protezione dei dati personali, con particolare riferimento a quelli adottati dal Garante Privacy italiano quali a titolo esemplificativo:

- Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015 ((Pubblicato sulla Gazzetta Ufficiale n. 179 del 4 agosto 2015);
- Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali - 13 ottobre 2008 (G.U. n. 287 del 9 dicembre 2008);
- Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali - 27 novembre 2008 (G.U. n. 287 del 9 dicembre 2008);
- Posta elettronica e internet - 1° marzo 2007;
- Le norme specifiche in materia di Privacy eventualmente applicabili al Responsabile (per esempio Regolamento e Privacy)
- ☐ Linee guida cookie e altri strumenti di tracciamento - 10 giugno 2021
- ☐ Provvedimento in materia di videosorveglianza - 8 aprile 2010;
- ☐ Adempimenti semplificati per il customer care (inbound) - 15 novembre 2007
- ☐ RFID Etichette intelligenti: prescrizioni - 9 Marzo 2005;
- ☐ Provvedimento generale prescrittivo in tema di biometria - 12 novembre 2014;
- ☐ Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro - 4 ottobre 2011;
- ☐ Sistemi di videosorveglianza per il controllo della procedura di raccolta del campione urinario a fini certificatori o di cura della salute - 15 maggio 2013;
- ☐ Trattamento di dati personali per profilazione on line - 19 marzo 2015;
- ☐ Trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati - 15 maggio 2014;
- ☐ Dossier sanitario - 4 giugno 2015
- ☐ Svolgimento di indagini di customer satisfaction in ambito sanitario - 5 maggio 2011;
- ☐ Le norme del Codice Privacy non in contrasto con il Regolamento Europeo e non oggetto di abrogazione/modifica
- ☐ per i trattamenti di dati sensibili svolti dai soggetti pubblici (quelli di cui all'art. 6.1.c) ed e) del GDPR), in considerazione dell'art. 6.2 del GDPR saranno valutate le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 del Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.
- ☐ Le buone prassi in materia di sicurezza o Privacy proposte da ENISA (Agenzia europea per la sicurezza delle reti e dell'informazione);

☐ Le buone prassi in materia di sicurezza o Privacy proposte da associazioni, a titolo esemplificativo:

- Center for Internet Security;
- Critical Security Controls for Effective Cyber Defense;
- CIS Benchmarks.

13) CERTIFICAZIONI PERTINENTI:

Per attestare l'adeguatezza delle misure di sicurezza adottate (cfr. art. 28.5 del GDPR), il Responsabile del trattamento aderisce a specifici codici di condotta o a schemi di certificazione come di seguito:

a) visto l'art. 43.1.b) del GDPR, che prevede una certificazione accreditata ISO 17065; considerato che ai fini del GDPR e quindi del presente affidamento/trattamento hanno una pertinenza "piena", il Responsabile del trattamento ha ottenuto il rilascio delle seguenti certificazioni:

- ☐ ISDP@10003 (ITA);
- ☐ Carpa (LU);
- ☐ Europrivacy (LU);
- ☐ Europrice (D);
- ☐ altra certificazione accreditata ISO 17065 in materia di protezione dei dati personali;

Commentato [9]: n. 10 punti ciascuna

b) analizzato l'art. 32 (nonché l'art. 25) del GDPR; considerato che la norma di accreditamento ISO 17021-1 non è da considerarsi valida ai fini del GDPR, e tuttavia molti argomenti trattati hanno riscontro in specifici requisiti di legge europei e nazionali; considerato che ai fini del presente affidamento sono considerate avere una pertinenza "accettabile", il Responsabile del trattamento possiede le seguenti certificazioni:

- ☐ ISO/IEC 27001;
- ☐ ISO/IEC 22301;
- ☐ ISO/IEC 20000-1;
- ☐ ISO/IEC 27701;
- ☐ ISO/IEC 27017 e ISO/IEC 27018, integrate, come addendum alla Norma ISO/IEC 27001;
- ☐ altra certificazione accreditata (e/o integrata) come addendum alla Norma ISO/IEC 27001;
- ☐ altra certificazione accreditata in materia di privacy e gestione della sicurezza delle informazioni;

Commentato [10]: n. 6 punti ciascuna

c) seppure ai fini del presente affidamento sono considerate avere una pertinenza "scarsa", il Responsabile del trattamento ha ottenuto le seguenti certificazioni:

- ☐ ISO 9001;
- ☐ ISO 13485;
- ☐ altra certificazione accreditata in materia di gestione della qualità;

Commentato [11]: n. 2 punti ciascuna

Commentato [12]: "Dispositivi medici - Sistemi di gestione per la qualità - Requisiti per scopi regolamentari"

d) infine, visto l'art. 106, comma 8, del D. Lgs. n. 36/2023, "Garanzie per la partecipazione alla procedura", sebbene abbiano una pertinenza "scarissima" in materia di protezione dei dati personali, ai fini del presente affidamento il Responsabile del trattamento ha ottenuto tra le norme di certificazione ivi previste le seguenti:

Commentato [13]: n. 1 punto ciascuna

Il responsabile del trattamento potrà descrivere in modo concreto le misure tecniche e organizzative specifiche e ulteriori che intende mettere in atto:

(Esempi di possibili misure adottate):

1. misure di pseudonimizzazione e cifratura dei dati personali;
2. misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
3. misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
4. procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento
5. misure di identificazione e autorizzazione dell'utente misure di protezione dei dati durante la trasmissione misure di protezione dei dati durante la conservazione
6. misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati misure per garantire la registrazione degli eventi
7. misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita misure di informatica interna e di gestione e governance della sicurezza informatica
8. misure di certificazione/garanzia di processi e prodotti misure per garantire la minimizzazione dei dati misure per garantire la qualità dei dati
9. misure per garantire la conservazione limitata dei dati misure per garantire la responsabilità
10. misure per consentire la portabilità dei dati e garantire la cancellazione

Per i trasferimenti a (sub-)responsabili del trattamento, descrivere anche le misure tecniche e organizzative specifiche che il (sub-)responsabile del trattamento deve prendere per essere in grado di fornire assistenza al titolare del trattamento.

Descrizione delle misure tecniche e organizzative specifiche che il responsabile del trattamento deve prendere per essere in grado di fornire assistenza al titolare del trattamento.

13) INFORMAZIONI SUL TRATTAMENTO E CONSENSO DELL'INTERESSATO:

L'informativa redatta dal Titolare del trattamento deve essere:

- ☐ Consegnata a mano all'interessato;
- ☐ Pubblicata online sul sito XXXX;
- ☐ Non applicabile;
- ☐ L'informativa redatta e consegnata dal Titolare stesso;

☐ Altro (specificare nello spazio sottostante).

Gestione del consenso.

Nell'eventualità in cui il trattamento fosse fondato sulla base giuridica del consenso "libero" dell'interessato, a quest'ultimo sarà fornita una specifica ed ulteriore nota di informazioni e gli sarà richiesto l'apposito consenso, in mancanza del quale non si procederà al relativo trattamento.

Il trattamento prevede la raccolta e registrazione del consenso tramite:

- ☐ Informativa e modulo raccolta consenso cartaceo redatto, reso e raccolto a cura del Titolare del trattamento;
- ☐ Informativa e modulo raccolta consenso cartaceo redatto a cura del Titolare e reso/raccolto da XXXX che dovrà consegnare la modulistica firmata al Titolare del trattamento;
- ☐ Raccolta e registrazione del consenso tramite sistema XXXX;
- ☐ Altro;
- ☐ Non applicabile.

—
—

ALLEGATO IV

Elenco dei *sub*-responsabili del trattamento

NOTA ESPLICATIVA:

Il presente allegato deve essere compilato in caso di autorizzazione specifica di *sub*-responsabili del trattamento [clausola 7.7, lettera a), opzione 1].

Il titolare del trattamento ha autorizzato il ricorso ai seguenti *sub*-responsabili del trattamento:

1. Nome:

Indirizzo:

Nome, qualifica e dati di contatto del referente:

Descrizione del trattamento (compresa una chiara delimitazione delle responsabilità qualora siano autorizzati più *sub*-responsabili del trattamento):

2.

Sub-responsabile del trattamento (Nome, ragione sociale, sede legale)	Luogo del trattamento	Attività svolte per conto del primo responsabile

ALLEGATO V

Elenco degli Amministratori di Sistema (AdS e AdS/L).

Le persone fisiche designate AdS sono individuate in base agli ampi criteri forniti nel provvedimento del Garante Privacy del 27 novembre 2008 [doc. web n. 1577499] (G.U. n. 300 del 24 dicembre 2008), come modificato in base al provvedimento del 25 giugno 2009, che considera come tali le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti nonché altre figure equiparabili quali gli amministratori di base dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Il Responsabile del trattamento qui di seguito annota gli estremi identificativi di tutti gli Amministratori di Sistema (AdS) nonché di quegli Amministratori di Sistema la cui attività riguarda anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori (AdS/L). Ciò anche al fine di consentire al Titolare di rendere nota o conoscibile l'identità degli AdS/L in relazione ai diversi servizi informatici cui questi sono preposti.

Il Responsabile tiene costantemente aggiornato tale allegato e informa specificamente per iscritto il Titolare del trattamento di eventuali modifiche previste di tale elenco riguardanti l'aggiunta o la sostituzione di Amministratori di Sistema.

Commentato [14]: [in alternativa] e in caso di accertamenti da parte del Garante o su richiesta del Titolare del trattamento, gli fornisce prontamente e comunque entro 24 ore il medesimo allegato

Col. 1 Cognome e Nome della persona fisica designata AdS	Col. 2 Società e Organizzazi one di appartenenz a	Col. 3 Ubicazion e di lavoro dell'AdS	Col. 4 Funzioni attribuite all'AdS: ambito di operatività per settori o per aree operative (<i>job description</i>)	Col. 5 Banca dati gestita e trattamenti consentiti	Col. 6 La persona in questione tratta informazioni di carattere personale dei lavoratori (AdS/L)?	
					SI	NO

Legenda:

Colonna 1: Cognome e Nome: cognome e nome della persona fisica che è stata designata, per iscritto, Amministratore di Sistema

Colonna 2: Organizzazione di appartenenza: indica la ragione sociale della Società di appartenenza dell'AdS e gli estremi identificativi dell'unità organizzativa nella quale l'AdS opera.

Colonna 3: Ubicazione: indica l'ubicazione di lavoro nella quale l'AdS svolge normalmente la sua attività

Colonna 4: Funzioni attribuite: descrive l'elenco dei servizi informatici assegnati alla persona, l'ambito di operatività per settori o per aree operativa. Vale a dire la *job description* dell'AdS.

Colonna 5: Banca dati gestita e trattamenti consentiti: indica le banche dati a cui l'AdS è autorizzato ad accedere e il tipo di operazioni consentite sui dati ivi contenuti. Vale adire il "profilo di autorizzazione" dell'AdS.

Colonna 6: Trattamento di informazioni dei lavoratori (AdS/L): la colonna "SI" indica quegli AdS la cui attività, in relazione ai diversi servizi informatici cui sono preposti, riguarda anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori (per brevità: "AdS/L"). Il dato viene fornito in adempimento a quanto prescritto dal Provvedimento del Garante che pone a carico dei Titolari del trattamento l'obbligo di rendere nota, nell'ambito della propria organizzazione, l'identità degli AdS/L al fine di richiamare l'attenzione sulla rilevanza e la criticità insite nello svolgimento della loro mansione.