Oggetto: **Atto di individuazione e nomina del Responsabile del trattamento dei dati ai sensi e per gli effetti dell'art. 28 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 - Regolamento Generale sulla Protezione dei Dati ("GDPR") e con rif. al Provvedimento a carattere generale dell'Autorità Garante Privacy del 27 Novembre 2008 e s.m.i, sulla figura dell'Amministratore di Sistema ("ADS").**

Il Cliente - come definito nel T&C cui il presente allegato si riferisce - in qualità di "Titolare del trattamento dei dati" (a seguire, per semplicità, "Titolare") ai sensi degli artt. 4 e 24 del Regolamento UE 2016/679 (a seguire, per semplicità, "GDPR") in persona del legale rappresentante pro-tempore

NOMINA
RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI E AMMINISTRATORE DI SISTEMA

iRoma S.r.l, di seguito anche "Responsabile del trattamento dei dati" (a seguire, per semplicità, "Responsabile"), ai sensi degli artt. 4 e 28 del GDPR, in persona del legale rappresentante pro-tempore.

PREMESSO CHE

- Si intende per:
  - **Titolare del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali (art. 4 GDPR);
  - **Responsabile del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (artt. 4 e 28 GDPR);
  - **Amministratore di Sistema (ADS):** figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali[1];
  - **Responsabile della Protezione dei Dati personali (RPD/DPO):** il DPO, figura storicamente già presente in alcune legislazioni europee, rappresenta un elemento fondante ai fini della responsabilizzazione, facilita l'osservanza della normativa e il margine competitivo delle imprese (si rinvia alla sez. 4 del GDPR e alle Linee guida del WP29 - WP243);
  - **Autorizzato / designato al trattamento:** chiunque acceda a determinate informazioni per svolgere specifici compiti e funzioni connessi al trattamento di dati personali sotto l'autorità del titolare del trattamento o del Responsabile del trattamento (artt. 29 GDPR e 2-quaterdecies D.lgs. 196/2003 armonizzato);
  - **Trattamento:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4 GDPR);
  - **Dati personali:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione,

[1] **N.B.** Ai fini del provvedimento in materia di ADS, vengono però considerate tali "*anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi*". Ancora, "*Attività tecniche quali il salvataggio dei dati (backup/recovery), l´organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un´effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, **anche quando l´amministratore non consulti "in chiaro" le informazioni medesime***". https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1577499

un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4 GDPR);

- **Dati particolari:** dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale (art. 9 GDPR);
- **Dati relativi a condanne penali e reati:** dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (art. 10 GDPR);
- **Accountability:** il principio di responsabilizzazione, insieme alle altre norme che disciplinano in modo più specifico le modalità di adempimento del GDPR e la ripartizione delle responsabilità, rende necessario definire i diversi ruoli dei vari soggetti coinvolti in un'attività di trattamento di dati personali.

- In forza del **rapporto esistente** tra Titolare e Responsabile (a seguire, "le Parti"), ai sensi dell'art. 28 del GDPR, il Responsabile che si intende designare con il presente atto svolge per conto del Titolare operazioni di trattamento di dati personali per le finalità specificate e nell'ambito delle attività connesse all'esecuzione del rapporto fra le Parti;
- Il Responsabile possiede l'esperienza, la capacità, l'affidabilità e fornisce idonee garanzie circa il pieno rispetto delle disposizioni vigenti in materia di trattamento dati personali, ivi compreso il profilo della sicurezza in relazione alle finalità e alle modalità delle operazioni di trattamento nonché alle garanzie di tutela dei diritti dell'interessato. Il Titolare, nella designazione del Responsabile, ha considerato anche le conoscenze specialistiche (fra cui le competenze tecniche in materia di misure di sicurezza e di violazione dei dati), il grado di affidabilità, la reputazione e le risorse di cui dispone;
- Al fine di meglio ottemperare al GDPR, e quindi per offrire la più idonea protezione dei dati e dei diritti dei soggetti interessati, le Parti intendono regolare, con il presente atto di nomina, i loro reciproci rapporti, senza che ciò comporti il riconoscimento di ulteriori compensi o rimborsi.

Tutto ciò premesso, che costituisce parte integrante del presente atto, le Parti convengono quanto segue.

OGGETTO DELL'ATTO DI NOMINA DEL
RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI E AMMINISTRATORE DI SISTEMA

In virtù del presente atto e del rapporto intercorrente tra le Parti, il Responsabile è autorizzato al trattamento dei dati qui di seguito puntualmente individuati per natura e finalità, tipologia e per categorie di interessati a cui si riferiscono e strettamente pertinenti alle attività svolte per conto del Titolare.

TIPOLOGIE DI DATI PERSONALI	CATEGORIE DI INTERESSATI	OGGETTO PRINCIPALE DEL TRATTAMENTO	NATURA DEL TRATTAMENTO E FINALITA' PERSEGUITE
☒ Dati personali: dati identificativi, anagrafici e di contatto, trattati dal responsabile nominato, anche in via potenziale / incidentale, nel contesto delle attività di assistenza e manutenzione alla piattaforma" Easy" ☒ Dati particolari: dati relativi alla salute, fermo restando che il Titolare del Trattamento rimane l'unico responsabile per l'individuazione della corretta causa giustificativa ai sensi dell'art. 9 GDPR	☒ Studenti (minorenni) e rispettivi famigliari/tutori ☒ Personale scolastico: insegnanti, educatori e altri collaboratori ☒ In generale, utenti della "piattaforma Easy"	☒ Fornitura della piattaforma "Easy" e relativa assistenza/supporto, come da T&C in essere tra le parti	☒ *la raccolta,* ☒ *la registrazione,* ☒ *l'organizzazione,* ☒ *la strutturazione,* ☒ *la conservazione,* *per il trattamento in oggetto il responsabile specifica che conserverà i dati trattati fno ad un massimo di 48 mesi dopo la scadenza della licenza in assenza di richiesta esplicita di cancellazione,* ☒ *l'adattamento o la modifica,* ☒ *l'estrazione,* ☒ *la consultazione,* ☒ *l'uso,* ☒ *la comunicazione mediante trasmissione,* ☐ *diffusione o qualsiasi altra forma di messa a disposizione,* ☒ *il raffronto o l'interconnessione,*

			☒ *la limitazione,* ☒ *la cancellazione o la distruzione.*

OBBLIGHI DEL RESPONSABILE

La sottoscrizione del presente atto vincola il Responsabile al Titolare del trattamento e fa sorgere in capo al Responsabile una serie di obblighi specificamente individuati in apposita e separata clausola che segue il presente documento (**Allegato A**). Al Responsabile non è consentito trattare i dati in modo diverso rispetto a quanto indicato nelle istruzioni del Titolare. Un responsabile del trattamento viola il GDPR qualora non si limiti a trattare i dati in base alle istruzioni del titolare del trattamento e inizi a definire mezzi e finalità propri. Il responsabile del trattamento sarà pertanto considerato titolare rispetto a tale ultimo trattamento e può essere soggetto a sanzioni qualora non si limiti a trattare i dati in base alle istruzioni impartite dal titolare del trattamento[2].

MISURE DI SICUREZZA E VIOLAZIONE DEI DATI

Il Responsabile è tenuto a mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio in merito al trattamento dei dati effettuato (art. 32 GDPR).

DECORRENZA – DURATA – CESSAZIONE DEL TRATTAMENTO

Il ruolo e le competenze assegnate al Responsabile del trattamento con il presente atto, hanno la medesima durata ed efficacia dell'accordo intercorrente tra le Parti e pertanto si intendono rinnovate ogni anno fino alla cessazione dell'accordo stesso o fino alla revoca da parte del Titolare.

Al termine del trattamento effettuato per conto del Titolare, il Responsabile deve, su istruzioni del Titolare del trattamento, restituire o cancellare i dati personali, e le relative copie esistenti, salvo che non siano previste specifiche e differenti politiche di conservazione dei dati (anche in relazione alle categorie di dati trattati) a norma del diritto dell'Unione o degli Stati membri cui è soggetto il Responsabile del trattamento. In entrambi i casi il Responsabile deve rilasciare contestualmente un'attestazione scritta che presso lo stesso non esiste alcuna copia dei dati personali trattati in nome e per conto del Titolare del trattamento.

ALLEGATI:

- *ALLEGATO A. obblighi del responsabile del trattamento designato e dei "subresponsabili" ex art. 28 e C81*
- *ALLEGATO B. misure di sicurezza e violazione dei dati*
- *ALLEGATO C. checklist misure di sicurezza – visionabile su richiesta*

ALLEGATO A.
OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO DESIGNATO E DEI "SUBRESPONSABILI" EX ART. 28 E C81

In virtù dell'atto che vincola il Responsabile designato al Titolare del trattamento, sorgono in capo al Responsabile una serie di obblighi.

1. **Rispetto delle istruzioni impartite dal/i Titolare/i:** Il Responsabile deve assistere e coadiuvare il Titolare nella corretta gestione delle operazioni di trattamento che dovranno esser effettuate nel pieno rispetto degli obblighi previsti dal GDPR. A tale proposito, il Responsabile deve trattare i dati personali soltanto su istruzione documentata del Titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o dello stato membro cui è soggetto il Responsabile del trattamento; in tal caso, il Responsabile deve informare il Titolare circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
2. **Riservatezza**: Il Responsabile deve assicurare per sé stesso e per le persone, da lui o dal Titolare del trattamento autorizzate al trattamento dei dati personali, piena riservatezza rispetto alle operazioni di trattamento effettuate.

[2] Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR, https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_it.pdf.

Sarà cura del Responsabile, qualora lo reputasse opportuno, vincolare le persone autorizzate al trattamento dei dati al segreto, mediante un adeguato obbligo legale di riservatezza, anche per il periodo successivo all'estinzione del rapporto di lavoro intrattenuto con il Responsabile, in relazione alle operazioni di trattamento da essi eseguite;

3. **Conformità a leggi e regolamenti applicabili:** Il Responsabile è tenuto ad uniformarsi alle disposizioni del GDPR e, più in generale, ad ogni altra disposizione normativa, nazionale e sovranazionale, attualmente in vigore o che in futuro venga a modificare, integrare o sostituire l'attuale disciplina applicabile in materia di trattamento dei dati personali. Il Responsabile è altresì tenuto a rispettare i provvedimenti a carattere generale dell'Autorità Garante competente e le linee guida adottate dall'European Data Protection Board (il Comitato Europeo per la Protezione dei Dati, a seguire "EDPB");
4. **Misure di sicurezza:** Prima dell'inizio del trattamento dei dati, il Responsabile è tenuto a mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio in merito al trattamento dei dati effettuato (art. 32 GDPR). A tal proposito si rinvia all'**Allegato B**, relativo alle misure di sicurezza e alla gestione di un'eventuale violazione dei dati personali trattati;
5. **Audit:** Il Responsabile del trattamento deve riferire al Titolare periodicamente e ogni volta che riceve una specifica richiesta in tal senso, i dettagli relativi all'adempimento di quanto disposto dal presente atto nonché dalla normativa privacy applicabile, o attraverso relazioni scritte o attraverso la compilazione di check list che verranno fornite.

   Inoltre, il Responsabile deve contribuire alle attività di revisione, comprese le ispezioni, e ad informare prontamente il Titolare del trattamento di ogni questione rilevante ai fini del presente mandato, quali, a titolo indicativo:
   - ✓ Istanze di interessati;
   - ✓ Richieste del Garante;
   - ✓ Esiti delle ispezioni;
   - ✓ Violazioni del GDPR o di altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati, o la messa in pericolo della riservatezza, dell'integrità e della disponibilità dei dati personali.
6. **Persone autorizzate al trattamento:** Il Responsabile si avvale di persone autorizzate al trattamento dei dati che operano sotto la sua responsabilità, alle quali fornisce specifiche istruzioni scritte (salvo che il diritto dell'Unione o degli Stati membri non richieda diversamente). È compito del Responsabile vigilare sulla corretta esecuzione di tali istruzioni.
7. **Responsabili di secondo livello o "Subresponsabili":** Il Titolare del trattamento autorizza il Responsabile del trattamento, individuato con il presente documento, a ricorrere ad un altro Responsabile (di seguito "Subresponsabile") per l'esecuzione di specifiche attività di trattamento.

   Il Responsabile inoltra al Titolare i nominativi e l'atto di nomina del "Subresponsabile" e lo informa di eventuali modifiche riguardanti l'aggiunta o la sostituzione di altri Responsabili, alle quali il Titolare del trattamento conserva il diritto di opporsi.

   Il Responsabile verifica periodicamente l'adeguatezza delle misure tecniche e organizzative di ciascun Sub-Responsabile autorizzato (anche mediante l'**Allegato D** alla presente nomina).

   Al "Subresponsabile" sono imposti, con specifico atto sottoscritto, gli stessi obblighi in materia di protezione dei dati contenuti nell'accordo che lega il Titolare e il Responsabile del trattamento. Il "Subresponsabile" è tenuto ad: osservare, valutare e organizzare la gestione del trattamento dei dati personali e la loro protezione (mettendo in atto tutte le misure tecniche ed organizzative adeguate per assicurare un livello di sicurezza adeguato al rischio derivante dal trattamento dati effettuato) affinché questi siano trattati in modo lecito e pertinente e nel rispetto della normativa vigente. Qualora il "Subresponsabile" del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del "Subresponsabile" anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" (ex art. 82 par. 3 GDPR).
8. **Rispetto del Provvedimento a carattere generale sugli Amministratori di Sistema dell'Autorità Garante Privacy del 27 Novembre 2008** (G.U. N. 300 Del 24 dicembre 2008) cosi come modificato dal Provvedimento a carattere generale dell'Autorità Garante Privacy del 25 giugno 2009 (G.U. N. 149 Del 30 giugno 2009)**:** Il Responsabile, ove applicabile garantirà al Titolare del trattamento che ciascun incaricato/autorizzato Amministratore di Sistema (ADS) accederà ai sistemi con proprio account utente e propria password singola.

   Con l'accettazione di questa nomina il Responsabile si impegna a:
   - ✓ nominare individualmente gli incaricati della propria organizzazione che rivestono il ruolo di Amministratori del Sistema informativo (ADS);

- ✓ garantire che la designazione ad ADS sia individuale e rechi l'elencazione analitica degli ambiti di operatività consentiti, in base al profilo di autorizzazione assegnato[3];
- ✓ fornire annualmente al Titolare del trattamento l'elenco aggiornato degli Amministratori di Sistema (nominativi) e verificare l'attività dei soggetti individuati, come prescritto dall'Autorità Garante[4];
- ✓ adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.
  Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi[5].

9. **Per eventuali trasferimenti di dati in Paesi ubicati al di fuori dello Spazio Economico Europeo (SEE)**. I dati personali dovranno rimanere in Paesi SEE. Solo previa autorizzazione scritta del Titolare, questi potranno essere trasferiti in Paesi extra SEE. Il trasferimento extra SEE, nel caso in cui sia accordato dal Titolare, dovrà avvenire in compliance con la normativa vigente e le Linee Guida dell'EDPB. Il Responsabile dovrà costantemente informare e aggiornare il Titolare sugli eventuali Paesi Extra SEE, sulle garanzie poste alla base del trasferimento dati e sulle eventuali ulteriori misure supplementari di garanzia poste in capo all'importatore.
10. **Registro dei Trattamenti:** Ove applicabile, il Responsabile deve tenere un Registro delle attività di trattamento svolte sotto la propria responsabilità in nome e per conto del Titolare del trattamento (art. 30 par. 2 GDPR). Il Registro, anche in formato elettronico, deve contenere tutta una serie di informazioni, che il Responsabile raccoglie anche interfacciandosi con i vari uffici o unità interne e/o esterne all'organizzazione, che trattano dati personali per conto del Titolare. Il Titolare potrebbe chiedere il registro del Responsabile per i trattamenti effettuati per suo conto.
11. **Esercizio dei diritti dell'interessato:** Il Responsabile dovrà informare tempestivamente e per iscritto il Titolare del trattamento circa la ricezione di eventuali richieste degli interessati, avanzate ai sensi degli artt. da 15 a 22 del GDPR, in merito, tra l'altro, alle finalità e alle modalità del trattamento, all'origine dei dati, all'aggiornamento, alla rettifica, cancellazione, portabilità, limitazione dei dati, all'opposizione al trattamento (compresa la profilazione), alla revoca del consenso prestato e/o all'intenzione di proporre reclamo al Garante per la protezione dei dati personali.
    In particolare, il Responsabile è tenuto a:
    - ✓ coordinarsi a tal fine con le funzioni preposte dal Titolare alle relazioni con i soggetti interessati;
    - ✓ attivare le dovute procedure atte a dare seguito alle richieste per l'esercizio dei diritti degli interessati, senza ingiustificato ritardo, e comunque, al più presto possibile dal ricevimento della richiesta stessa.
12. **Altri adempimenti:** il Responsabile del trattamento è altresì tenuto a:
    - ✓ cooperare con l'Autorità di Controllo quando richiesto;
    - ✓ supportare l'attività svolta dal DPO (Data Protection Officer – Responsabile della Protezione dei Dati) per conto del Titolare del trattamento, se nominato (artt. 37 e ss. GDPR);
    - ✓ designare per iscritto un Rappresentante che lo rappresenti nell'Unione, se il Responsabile non è stabilito nell'UE e ricorrano i presupposti di cui all'art. 27 del GDPR.

ELENCO DEI SUBRESPONSABILI DEL RESPONSABILE, SE PRESENTI:

Non Presenti.

ALLEGATO B.
MISURE DI SICUREZZA E VIOLAZIONE DEI DATI
(sezione 2 del GDPR e C. 83, 85, 86, 87, 88)

[3] "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008"*, paragrafo 4.2.
[4] "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008"*, paragrafo 4.3 e 4.4.
[5] "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008"*, paragrafo 4.5.

Misure di sicurezza. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Responsabile del trattamento deve mettere in atto misure tecniche e organizzative adeguate per assicurare un livello di sicurezza adeguato al rischio, previste dall'art. 32 GDPR, che comprendono, tra le altre, se del caso:

- **a)** la pseudonimizzazione e la cifratura dei dati personali;
- **b)** la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- **c)** la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- **d)** una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Tali misure devono assicurare un elevato livello di sicurezza, essere costantemente aggiornate e rivalutate periodicamente in relazione ai rischi (che possono variare nel tempo). Nella valutazione del rischio per la sicurezza dei dati, il Responsabile del trattamento deve tenere in considerazione i rischi presentati dal trattamento dei dati personali come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.
Ulteriori eventuali disposizioni di dettaglio sugli obiettivi di sicurezza da raggiungere, e sulle specifiche misure di sicurezza da implementare, potranno anche essere fornite a parte, mediante corrispondenza o pareri contenenti istruzioni.

Obblighi di assistere. Il Responsabile del trattamento, se necessario e su richiesta, dovrà assistere il Titolare:

- ✓ nell'adempimento dell'obbligo di adottare misure tecniche e organizzative adeguate per garantire la sicurezza del trattamento;
- ✓ nell'adempimento dell'obbligo di notificare le violazioni dei dati personali all'autorità di controllo e agli interessati (v. disposizioni di dettaglio a seguire);
- ✓ nella redazione del "DPIA" (*Data Protection Impact Assessment),* contenente la valutazione sulla particolare probabilità e gravità del rischio inerente alle operazioni di trattamento da effettuare (tenuto conto della natura, dell'ambito di applicazione, del contesto, delle finalità e delle fonti di rischio) e sulle misure tecniche ed organizzative da adottare al fine di attenuare tale rischio, assicurando la protezione dei dati personali e la conformità al GDPR. Se del caso, il Responsabile dovrà richiedere un parere in merito al DPO (*Data Protection Officer*), se nominato (art.35 e C.90 GDPR);
- ✓ nell'eventuale consultazione all'autorità di controllo, qualora il risultato del DPIA indichi la sussistenza di un rischio elevato che non può essere attenuato.

Violazione dei dati. Se dovesse venire a conoscenza di una violazione dei dati personali (*Data Breach*), il Responsabile, senza ingiustificato ritardo, deve informare per iscritto il Titolare del trattamento affinché possa procedere, se del caso, a notificare la violazione all'autorità di controllo competente (art. 33 GDPR) e, qualora la violazione dei dati personali in questione dovesse essere suscettibile di presentare un elevato rischio per i diritti e le libertà delle persone fisiche, il Titolare del trattamento provvederà a darne comunicazione all'interessato (art. 34 GDPR).
Il Responsabile deve coadiuvare il Titolare del trattamento per individuare prontamente le violazioni dei dati subite (*Data Breaches*) e avere una policy/procedura con linee guida riguardanti:

- ✓ la valutazione della violazione subita, al fine di individuare i rischi per i diritti e le libertà delle persone fisiche, stimarne la relativa gravità e determinare se il *breach* necessita di essere notificato o meno all'Autorità di controllo competente;
- ✓ la scelta delle informazioni da fornire all'interessato attraverso la comunicazione della violazione, nel caso in cui, dalla valutazione di cui al punto precedente, il *breach* presenti rischi elevati per i diritti e le libertà delle persone fisiche coinvolte.

Il Responsabile dovrà aiutare il Titolare del trattamento a documentare per iscritto qualsiasi violazione di dati subita, le circostanze ad essa relative, le conseguenze e i provvedimenti adottati per porvi rimedio.
Nello specifico dovranno essere documentati:

a) la natura della violazione dei dati personali, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati personali oggetto di violazione;
b) il nome e i dati di contatto del DPO (se nominato) o di un altro punto di contatto presso cui l'Autorità di controllo competente potrà ottenere maggiori informazioni;
c) le probabili conseguenze della violazione dei dati personali;

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

Tale documentazione dovrà essere resa disponibile all'Autorità di controllo competente attraverso la procedura di notifica della violazione dei dati (*Data breach)* prevista dall'art. 33 par. 3 del GDPR.