**Valutazione di Impatto**

**PROGETTO/SERVIZIO/PROCEDIMENTO <denominazione>**

Autore: <nominativo autore>

Valutatore: <nominativo attuale RPD> (RPD-CNR)

Validatore: <Responsabile Interno ex art. 19 ROF CNR>

**Contesto**

**Panoramica del trattamento**

**Quale è il trattamento in considerazione?**

*[descrivere il trattamento]*

**Quali sono le responsabilità connesse al trattamento?**

*[Indicare Titolare/i, eventuale/i Responsabile/i ex art. 28 GDPR, personale incaricato. In caso di più titolari, indicare se si tratta di titolari autonomi o contitilari].*

**Ci sono standard applicabili al trattamento?**

*[indicare se si applicano particolari standard, linee guida, codici di condotta, regole deontologiche, norme, etc. relativi alla materia specifica del trattamento.*

*Di seguito alcuni esempi a mero titolo illustrativo:*

* *Carta dei Diritti Fondamentali dell’Unione Europea;*
* *Regolamento generale sulla protezione dei dati (Regolamento UE 2016/679);*
* *Decreto legislativo 30/06/2003 n. 196 (Codice novellato);*
* *Prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell’articolo 21, comma 1 del decreto legislativo 10 agosto 2018, n. 101 (Provvedimento n. 146/2019);*
* *Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell’art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018;*
* *Provvedimento CNR n. 27/2019, Compiti e funzioni dei Responsabili interni CNR in materia di Trattamento dei dati personali;*
* *Codice di comportamento del CNR, 2017 (Deliberazione C.d.a. n. 137/2017);*
* *Guidelines 07/2020 on the concepts of controller and processor in the GDPR, del Comitato europeo per la protezione dei dati;*
* *Guidelines 05/2020 on consent under Regulation 2016/679, del Comitato europeo per la protezione dei dati;*
* *Linee guida per l’integrità nella ricerca, della Commissione per l’Etica e l’Integrità nella Ricerca del CNR.]*

**Dati, processi e risorse di supporto**

**Quali sono i dati trattati?**

*[Indicare le tipologie di dati (identificativi, comuni, particolari, giudiziari, etc.) e per ciascuna categoria indicare in dettaglio i dati trattati].*

**Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?**

*[descrive le fasi del ciclo di vita dei dati]*

**Fase 1 - <nome breve della fase>:** …

**Fase 2 - <nome breve della fase>:** …

**Fase 3 - <nome breve della fase>:** …

**Fase 4 - <nome breve della fase>:** …

…

**Quali sono le risorse di supporto ai dati?**

*[Indicare le piattaforme, gli strumenti e i supporti per il trattamento e la conservazione dei dati]*

**Principi Fondamentali**

**Proporzionalità e necessità**

**Gli scopi del trattamento sono specifici, espliciti e legittimi?**

*[Indicare gli scopi dei trattamenti dimostrando che sono specifici, espliciti e legittimi]*

**Quali sono le basi legali che rendono lecito il trattamento?**

*[Indicare le basi giuridiche del trattamento - vd artt. 6, 9 e 10 del GDPR]*

**I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?**

*[Dimostrare che viene trattato un insieme minimo di dati rispetto alle finalità legittimamente perseguite]*

**I dati sono esatti e aggiornati?**

*[Descrivere le misure messe in atto per garantire l’aggiornamento dei dati personali trattati]*

**Qual è il periodo di conservazione dei dati?**

*[Indicare periodo di conservazione in termini puntuali o tramite un criterio oggettivo per individuarli]*

**Misure a tutela dei diritti degli interessati**

**Come sono informati del trattamento gli interessati?**

*[Indicare modalità attraverso le quali viene resa l’informativa agli interessati]*

**Ove applicabile: come si ottiene il consenso degli interessati?**

*[Se il trattamento è basato sul consenso, indicare le modalità attraverso le quali è ottenuto]*

**Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?**

*[Indicare in modo puntuale le modalità attraverso le quali gli interessati possono esercitare il diritto di portabilità dei dati]*

**Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all’oblio)?**

*[Indicare in modo puntuale le modalità attraverso le quali gli interessati possono esercitare il diritto di cancellazione dei dati]*

**Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?**

*[Indicare in modo puntuale le modalità attraverso le quali gli interessati possono esercitare i diritti di limitazione e opposizione al trattamento dei dati]*

**Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?**

*[Nel caso in cui sia nominato un Responsabile Esterno ex art. 28 del GDPR, indicarne gli estremi e specificarne i contenuti. Se possibile, allegarne copia*

*]*

**In caso di trasferimento di dati al di fuori dell’Unione europea, i dati godono di una protezione equivalente?**

*[Specificare se i dati personali vengono trasferiti in paesi extra UE e, in caso affermativo, specificare le tutele applicate – es. esiste una decisione di adeguatezza emanata dalla Commissione Europea in merito alla normativa del paese extra UE]*

**Rischi**

**Misure esistenti o pianificate**

**Crittografia**

*[Indicare se è utilizzata la crittografia e, in caso affermativo, specificare l’algoritmo e le modalità di applicazione]*

**Pseudonimizzazione**

*[Eventuali misure di pseudonimizzazione]*

**Anonimizzazione**

*[Eventuali misure di anonimizzazione]*

**Archiviazione**

*[Specificare misure di sicurezza relative all’archiviazione dei dati]*

**Sicurezza dei siti web**

*[Specificare misure di sicurezza relative ad eventuali siti web]*

**Sicurezza delle postazioni**

*[Specificare misure di sicurezza relative alle postazioni di lavoro tramite le quali vengono trattati i dati personali]*

**Manutenzione**

*[Specificare criteri e frequenza della manutenzione di piattaforme, dispositivi e supporti]*

**Lotta contro il malware**

*[Specificare le misure di lotta al malware – es. antivirus]*

**Controllo degli accessi logici**

*[Specificare le misure di controllo degli accessi logici]*

**Minimizzazione dei dati**

*[Illustrare le motivazioni per cui i dati trattati sono solo quelli strettamente necessari per le finalità lecite del trattamento]*

**Contratto con il responsabile del trattamento**

*[Specificare le previsioni dell’eventuale contratto con il responsabile esterno ex art. 28 per mitigare i rischi]*

**Sicurezza dei canali informatici**

*[Illustrare misure per la sicurezza di rete e di eventuali altri canali di comunicazione dei dati]*

**Controllo degli accessi fisici**

*[Illustrare misure per il controllo degli accessi fisici ai locali in cui sono conservati/gestiti i dati personali]*

**Sicurezza dei documenti cartacei**

*[Illustrare misure per la sicurezza dei documenti cartacei]*

**Tracciabilità**

*[**Illustrare misure per il tracciamento delle operazioni di trattamento]*

**Protezione contro fonti di rischio non umane**

*[Indicare misure di protezione da eventi naturali quali incendi, allagamenti, fenomeni climatici straordinari o da altre fonti di rischio non umane].*

**Politica di tutela della privacy**

*[Illustrare l’organizzazione privacy dell’Ente e della/e struttura/e che trattano i dati – vd ROF e provv. 27/2029 del Presidente CNR]*

**Backup**

*[Illustrare frequenza e criteri di backup dei dati]*

**Gestione degli incidenti di sicurezza e delle violazioni di dati personali**

*[Illustrare politiche e modalità di gestione degli incidenti e delle violazioni]*

**Gestione del personale**

*[Modalità di autorizzazione e formazione del personale autorizzato]*

**Accesso illegittimo ai dati**

**Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?**

*[Descrivere gli effetti negativi che si potrebbero concretizzare in relazione ai diritti, alle libertà e agli interessi legittimi degli interessati]*

**Quali sono le principali minacce che potrebbero concretizzare il rischio?**

*[Specificare le potenziali minacce – es. errore umano, intrusione informatica, comportamenti sleali del personale autorizzato]*

**Quali sono le fonti di rischio?**

*[Indicare le potenziali fonti del rischio – es. fonti umane interne, fonti umane esterne, …]*

**Quali misure fra quelle individuate contribuiscono a mitigare il rischio?**

* …
* …

**Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?**

Trascurabile/Limitato/Importante/Massimo

*[Motivare]*

**Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?**

Trascurabile/Limitato/Importante/Massimo

*[Motivare]*

**Modifiche indesiderate dei dati**

**Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?**

*[Descrivere gli effetti negativi che si potrebbero concretizzare in relazione ai diritti, alle libertà e agli interessi legittimi degli interessati]*

**Quali sono le principali minacce che potrebbero concretizzare il rischio?**

*[Specificare le potenziali minacce – es. errore umano, intrusione informatica, comportamenti sleali del personale autorizzato]*

**Quali sono le fonti di rischio?**

*[Indicare le potenziali fonti del rischio – es. fonti umane interne, fonti umane esterne, …]*

**Quali misure fra quelle individuate contribuiscono a mitigare il rischio?**

* …
* …

**Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?**

Trascurabile/Limitato/Importante/Massimo

*[Motivare]*

**Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?**

Trascurabile/Limitato/Importante/Massimo

*[Motivare]*

**Perdita di dati**

**Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?**

*[Descrivere gli effetti negativi che si potrebbero concretizzare in relazione ai diritti, alle libertà e agli interessi legittimi degli interessati]*

**Quali sono le principali minacce che potrebbero concretizzare il rischio?**

*[Specificare le potenziali minacce – es. errore umano, intrusione informatica, comportamenti sleali del personale autorizzato]*

**Quali sono le fonti di rischio?**

*[Indicare le potenziali fonti del rischio – es. fonti umane interne, fonti umane esterne, …]*

**Quali misure fra quelle individuate contribuiscono a mitigare il rischio?**

* …
* …

**Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?**

Trascurabile/Limitato/Importante/Massimo

*[Motivare]*

**Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?**

Trascurabile/Limitato/Importante/Massimo

*[Motivare]*