CONSIGLIO REGIONALE DEL LAZIO

Direzione: SERVIZIO PREVENZIONE CORRUZIONE, TRASPARENZA

Area:

DETERMINAZIONE *(con firma digitale)*

N. A00062 **del** 24/02/2023 **Proposta n.** 202 **del** 13/02/2023

Oggetto:

Adempimenti ex regolamento (UE) 2016/679. Art. 418 bis, co. 1 del regolamento di organizzazione del Consiglio regionale. Istituzione del "Nuovo Registro delle attività di trattamento dei dati personali". Adozione di una scheda/format per il censimento e la qualificazione dei dati personali.

Proponente:

Estensore	CRISTIANA GIORDANO	_____*firma elettronica*_____
Responsabile del procedimento	CRISTIANA GIORDANO	_____*firma elettronica*_____
Responsabile dell' Area		_____
Direttore	DOMINICI BARBARA	_____*firma digitale*_____

Firma di Concerto

Richiesta di pubblicazione sul BUR: NO

OGGETTO: *Adempimenti ex regolamento (UE) 2016/679. Art. 418 bis, co. 1 del regolamento di organizzazione del Consiglio regionale. Istituzione del "Nuovo Registro delle attività di trattamento dei dati personali". Adozione di una scheda/format per il censimento e la qualificazione dei dati personali.*

La Direttrice

VISTO lo Statuto, approvato con legge statutaria 11 novembre 2004, n. 1 e successive modifiche e, in particolare, gli articoli 24 e 53;

VISTO il decreto legislativo 30 marzo 2001, n. 165 (Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche) e successive modifiche;

VISTA la legge regionale 18 febbraio 2002, n. 6 (Disciplina del sistema organizzativo della Giunta e del Consiglio e disposizioni relative alla dirigenza ed al personale regionale) e successive modifiche;

VISTO il regolamento di organizzazione del Consiglio regionale, approvato con deliberazione dell'Ufficio di presidenza 29 gennaio 2003, n. 3 e successive modifiche, di seguito "regolamento di organizzazione";

VISTA la determinazione 9 febbraio 2022, n. A00138 (Istituzione delle aree presso il Consiglio regionale del Lazio. Revoca della determinazione 2 settembre 2021, n. 107);

VISTO il decreto del Presidente del Consiglio regionale 20 febbraio 2020, n. 3, con il quale, previa deliberazione dell'Ufficio di presidenza 9 gennaio 2020, n. 1, alla sottoscritta dott.ssa Barbara Dominici è stato conferito l'incarico di direttore del servizio "Prevenzione della corruzione, Trasparenza";

VISTA la legge 7 agosto 1990, n. 241 (Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi) e successive modifiche;

VISTO il 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), di seguito "regolamento (UE)", e, in particolare, l'articolo 30 (Registri delle attività di trattamento);

VISTO il decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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) e successive modifiche;

VISTO l'articolo 418 bis (Registri delle attività di trattamento e delle violazioni dei dati personali), comma 1 del regolamento di organizzazione, così come sostituito dalla deliberazione dell'Ufficio di presidenza 27 febbraio 2019, n. 39 (Approvazione modifiche al regolamento di organizzazione del Consiglio regionale in materia di privacy e alle "Linee guida per il trattamento dei dati personali" di cui alla propria deliberazione n. 60/2018), ai sensi del quale:
"1. *Il direttore del servizio Prevenzione della corruzione, Trasparenza con proprio provvedimento, sentito il segretario generale, istituisce, in conformità con quanto previsto dagli articoli 30 e 33, paragrafo 5. del RGPD, rispettivamente il registro delle attività di trattamento dei dati personali e il registro delle violazioni dei dati personali, che sono tenuti, sia in formato cartaceo che in formato elettronico, dalla struttura organizzativa, all'interno dello stesso servizio, competente in materia di tutela della privacy.*"

CONSIDERATO che:

- il richiamato articolo 418 bis del regolamento di organizzazione prevedeva, prima della modifica di cui al paragrafo precedente, che il registro delle attività di trattamento dei dati personali, di seguito "registro delle attività di trattamento", fosse istituito con determinazione del segretario generale;
- in coerenza con quanto evidenziato nel capoverso precedente il segretario generale, con determinazione 24 maggio 2018, n. 349, provvedeva a istituire il registro delle attività di trattamento;
- successivamente all'istituzione del registro delle attività di trattamento di cui al capoverso precedente sono state adottate diverse e sostanziali modifiche dell'assetto organizzativo del Consiglio regionale, concernenti sia le strutture apicali sia quelle incardinate nelle stesse, con conseguenti variazioni delle relative declaratorie di competenza (deliberazioni dell'Ufficio di presidenza: 9 gennaio 2019, n. 1; 5 agosto 2021, n. 57; 27 gennaio 2022, n. 10 - corrispondenti determinazioni del segretario generale: 22 gennaio 2019, n. 54; 2 settembre 2021, n. 107; 9 febbraio 2022, n. A00138);
- con deliberazione dell'Ufficio di presidenza 18 maggio 2022, n. 46 (Piano della prestazione e dei risultati del Consiglio regionale per il triennio 2022-2024, Piano triennale delle azioni positive per il triennio 2022-2024 e Programmazione del lavoro agile e delle sue modalità di attuazione e sviluppo vigente fino alla definizione del Piano integrato di attività e organizzazione (PIAO)), nell'ambito dell'obiettivo strategico n. 1.2 - Valorizzazione del ruolo istituzionale del Consiglio regionale, è stato individuato l'obiettivo, comune a tutte le attuali strutture organizzative, "Certificazione di qualità UNI ISO 9001 del Consiglio regionale";
- la realizzazione dell'obiettivo di cui al capoverso precedente ha richiesto, preliminarmente, la definizione della mappatura dei processi e subprocessi di competenza delle diverse strutture in cui si articola il vigente assetto organizzativo del Consiglio regionale, in una duplice ottica: l'individuazione (mappatura) dei rischi e delle misure di sicurezza inerenti all'anticorruzione; l'individuazione (mappatura) delle attività di trattamento dei dati personali e, consequenzialmente, delle misure di sicurezza a esse corrispondenti;
- la ricordata procedura di conseguimento della "Certificazione di qualità UNI ISO 9001 del Consiglio regionale" si è conclusa nel mese di dicembre 2022;

— a seguito di detta mappatura dei processi e subprocessi si presenta l'esigenza di procedere, come prima evidenziato, a un nuovo censimento (mappatura) delle attività che prevedano, nell'ambito dei processi/subprocessi stessi, il trattamento di dati personali;

RITENUTO, alla luce di quanto avanti esposto, di procedere, in conformità con quanto previsto dall'articolo 30 del regolamento (UE) e dall'articolo 418 bis, comma 1 del regolamento di organizzazione, all'istituzione di un nuovo registro delle attività di trattamento secondo lo schema di cui all'Allegato A (Nuovo Registro delle attività di trattamento dei dati personali) alla presente determinazione, da compilare con le informazioni raccolte in base all'Allegato B alla presente determinazione (Scheda/format per il censimento e la qualificazione dei dati personali), allegati che costituiscono parti integranti e sostanziali della stessa;

SENTITO la segretaria generale in merito ai documenti cui al paragrafo precedente;

RITENUTO di:

— far coincidere l'efficacia del Nuovo Registro delle attività di trattamento dei dati personali, di cui all'Allegato A alla presente determinazione, con la data di formale presa d'atto, da parte del direttore *pro tempore* del servizio Prevenzione della corruzione, Trasparenza, della sua avvenuta completa compilazione, con la conseguenza che fino a tale data resta valido il registro delle attività di trattamento istituito con la richiamata determinazione n. 349/2018;
— revocare la determinazione n. 349/2018 a decorrere dalla data di presa d'atto di cui al capoverso precedente;

DETERMINA

per i motivi espressi in premessa, che costituiscono parte integrante e sostanziale della presente determinazione

1. di procedere:
    a) all'istituzione del Nuovo Registro delle attività di trattamento dei dati personali, secondo lo schema riportato nell'Allegato A (Nuovo Registro delle attività di trattamento dei dati personali) alla presente determinazione, di cui costituisce parte integrante e sostanziale;
    b) all'adozione della Scheda/format per il censimento e la qualificazione dei dati personali, riportato nell'allegato B alla presente determinazione, di cui costituisce parte integrante e sostanziale, funzionale alla compilazione del documento di cui alla lettera a);
2. di:
    a) far coincidere l'efficacia del Nuovo Registro delle attività di trattamento dei dati personali di cui al punto 1, lettera a), con la data di formale presa d'atto, da parte del direttore *pro tempore* del servizio Prevenzione della corruzione, Trasparenza, della sua avvenuta completa compilazione, con la conseguenza che fino a tale data resta valido il registro delle attività di trattamento istituito con la determinazione, richiamata in premessa, n. 349/2018;
    b) revocare la determinazione n. 349/2018 a decorrere dalla presa d'atto di cui alla lettera a);

3. di stabilire che il Nuovo Registro delle attività di trattamento dei dati personali di cui al punto 1, lettera a) sarà tenuto, sia in formato cartaceo sia in formato elettronico, dalla struttura competente in materia di tutela della *privacy*;
4. di trasmettere, in via telematica, la presente determinazione alla Segretaria generale, ai direttori dei servizi e al Responsabile della protezione dei dati personali (RPD) del Consiglio regionale, ciascuno per gli adempimenti di competenza;
5. di pubblicare la presente determinazione nella sezione "Amministrazione trasparente" del sito *web* istituzionale del Consiglio regionale.

Dott.ssa Barbara Dominici

Allegato A alla determinazione ……. n. …

Nuovo Registro delle attività di trattamento dei dati personali (art. 30, par. 1 del regolamento (UE) 2016/679)

Titolare del Trattamento:

Dati di contatto:

Contitolare del trattamento:

Dati di contatto:

Responsabile della Protezione dei dati (RPD):

Dati di contatto::

N.	Struttura organizzativa	Attività di trattamento	Finalità e base giuridica (art. 30, par. 1, lett. b) del regolamento (UE) 2016/679)	Fonti del trattamento

Categoria dati (art. 30, par. 1, lett. c) del regolamento (UE) 2016/679)	Categoria interessati e categoria destinatari (art. 30, par. 1, lett. c) e d) del regolamento (UE) 2016/679)	Banche dati associate al trattamento	Misure di sicurezza (art. 30, par. 1, lett. g) del regolamento (UE) 2016/679)	Termini di cancellazione (art. 30, par. 1, lett. f) del regolamento (UE) 2016/679)

CONSIGLIO
REGIONALE
DEL LAZIO

ALLEGATO B

"Nuovo Registro delle attività di trattamento dei dati personali":
Scheda/format per il censimento e la qualificazione dei dati personali

NOTE PER LA COMPILAZIONE

Per i riferimenti normativi al regolamento UE 2016/679 (GDPR - General Data Protection Regulation), di seguito RGPD, contenuti nella presente scheda, è possibile consultare la seguente risorsa: www.privacy-regulation.eu/it/index.htm.
I campi evidenziati in rosso costituiscono elementi informativi obbligatori del registro dei trattamenti.

ELEMENTI IDENTIFICATIVI DELLA SCHEDA DI TRATTAMENTO

Struttura organizzativa competente per le attività di trattamento	
Nominativo del responsabile della struttura organizzativa nella sua qualità di "delegato al trattamento[1]" (di seguito "delegato")	
Nominativo del soggetto compilatore della scheda nella sua qualità di "persona autorizzata al trattamento[2]" (di seguito "persona autorizzata")	

ELEMENTI IDENTIFICATIVI DEL TRATTAMENTO

Denominazione dell'attività di trattamento[3]	
Tipologia di dati personali oggetto di trattamento	☐ Dati personali[4] ☐ Dati personali appartenenti a categorie particolari (ex dati sensibili)[5]

1 Cfr. l'art. 411 bis, co. 1 del regolamento di organizzazione del Consiglio regionale, approvato con deliberazione dell'Ufficio di presidenza 29 gennaio 2003, n. 3 e successive modifiche, di seguito regolamento di organizzazione, che recita:
"I delegati al trattamento dei dati personali, di seguito denominati Delegati, conformemente con gli articoli 28 e 29 del RGPD, sono i dirigenti e i titolari di incari-chi di funzione dirigenziale, comunque denominati, che comportano l'esercizio delle competenze di amministrazione e gestione, ciascuno per la parte di propria competenza.".

2 Cfr. l'art. 411 bis del regolamento di organizzazione che recita:

- *"Le persone autorizzate al trattamento dei dati personali, di seguito denominati Persone autorizzate, conformemente con gli articoli 4, paragrafo 1., numero 10) e 28, paragrafo 3., lettera b) del RGPD, sono i dipendenti formalmente autorizzati al trattamento di dati personali dai Delegati, con specifica individuazione dell'ambito del trattamento consentito, sul presupposto dell'assegnazione alla relativa struttura organizzativa." (co. 3);*
- *"I Delegati e le Persone autorizzate provvedono al trattamento di dati personali nei termini e con le modalità di cui alle relative disposizioni del RGPD e coerente-mente con le previsioni contenute in apposite linee guida approvate dall'Ufficio di presidenza." (co. 4).*

3 Poiché la mappatura delle singole attività di trattamento discende dalla mappatura dei processi/subprocessi che comportano attività di trattamento di dati personali, la "denominazione" in parola coincide ordinariamente con la finalità perseguita con l'attività di trattamento stessa. A tale ultimo riguardo, si ricorda che a norma dell'art. 4, par. 2, del RGPD, per "*trattamento*" si intende: *"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;"*

4 Cfr. l'art. 4, par. 1 del RGPD secondo il quale per *"dato personale"* si intende *"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, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.".*

5 Cfr. l'art. 9, par. 1 del RGPD secondo il quale per "*categorie particolari di dati personali*" si intendono quei dati che "*rivelino l'origine*

	☐ Dati personali relativi a reati, condanne…..[6](ex dati giudiziari)
Tipologia di dati appartenenti a categorie particolari ex art. 9 del RGPD (già "dati sensibili")	☐ origine razziale o etnica ☐ opinioni politiche ☐ convinzioni religiose o filosofiche ☐ appartenenza sindacale ☐ stato di salute ☐ vita o orientamento sessuale ☐ dati genetici ☐ dati biometrici
Tipologia di dati relativi a condanne penali e reati ex art. 10 del RGPD (già "dati giudiziari"[7])	☐ condanne penali ☐ reati (carichi pendenti ad esempio: indagato/imputato) ☐ provvedimenti cautelari ☐ misure di sicurezza ☐ sanzione amministrativa dipendente da reato.
Categoria di interessati[8]	
Finalità del trattamento[9]	
Base giuridica per il trattamento di dati personali[10]	
Base giuridica per il trattamento di dati ex art. 9 RGPD (già "dati sensibili")[11]	
Base giuridica per il trattamento di dati ex art. 10 RGPD (già "dati giudiziari")	

RUOLO DEL CONSIGLIO REGIONALE DEL LAZIO AI FINI DEL TRATTAMENTO

Ruolo del Consiglio regionale ai fini del trattamento	☐ Titolare del trattamento[12] ☐ Contitolare del trattamento[13]

razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, 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.".

6 Cfr. l'art. 10 del RGPD secondo il quale per "*dati giudiziari*" si intendono quelli "*relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1* (omissis).".

7. I dati giudiziari, si tratta di dati relativi alle condanne penali e ai reati (carichi pendenti ad esempio: indagato/imputato) o a provvedimenti cautelari, misure di sicurezza e quindi idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti nonché la qualità di indagato o imputato. Riportare la specifica normativa (nazionale o dell'Unione europea) che ne autorizza il trattamento ai sensi dell'art. 10 del RGPD.

8. La persona fisica identificata o identificabile cui fanno riferimento i dati personali (es., dipendenti, cittadini, fornitori…).

9 La finalità consiste nella motivazione per cui vengono trattati i dati, es.: gestione del rapporto di lavoro (per i dati dei dipendenti).

10 Individuarne tra quelle di cui all'Art. 6 RGPD; qualora il trattamento si basi sulla lett. c) "obbligo legale" od e) "interesse pubblico o esercizio di pubblici poteri", indicare la specifica normativa (di rango costituzionale, primario o secondario) che rende necessario o autorizza il trattamento stesso. PS: la base giuridica di cui alla lett. f) "interesse legittimo" del titolare, non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

11 Sceglierne almeno una tra quelle di cui all'art. 9, par. 2 RGPD.

12 Cfr. l'art. 4, n. 7 RGPD secondo il quale per "*titolare del trattamento*" si intende: *" 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.".*

13 Cfr. l'art. 26, par. 1 RGPD secondo il quale per "*contitolare del trattamento*" si intende: "*Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento.* (omissis).".

	☐ Responsabile del trattamento[14]
In caso di contitolarità, indicare nome e dati di contatto dell'altro/degli altri titolare/i e gli estremi dell'accordo ex art. 26 RGPD stipulato[15]	
In caso di responsabilità del trattamento ex art. 28 RGPD, indicare nome e dati di contatto del titolare e gli estremi del contratto/atto giuridico ex art. 28 RGPD stipulato[16]	

DEFINIZIONE DEL CICLO DI VITA DEI DATI PERSONALI OGGETTO DI TRATTAMENTO

I dati oggetto di trattamento sono acquisiti:	☐ direttamente dagli interessati	
	☐ da altre strutture/organi interni al Consiglio	*(indicare quali)*
	☐ da soggetti (enti, organizzazioni, autorità, entità o persone fisiche diversi dall'interessato) esterne al Consiglio	*(indicare quali)*
In caso di raccolta diretta presso gli interessati:	è resa l'informativa ex art. 13 RGPD ☐ sì ☐ no	
Nel caso in cui i dati non siano ottenuti direttamente dall'interessato	è resa l'informativa ex art. 14 RGPD ☐ sì ☐ no	

14 Cfr. l'art. 28 RGPD secondo il quale per "responsabile *del trattamento*" si intende: "*Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.*".

15 Cfr. l'art. 26, par. 1 RGPD secondo il quale *"due o più titolari del trattamento determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati. (omissis)."*

16 Cfr. l'art. 28 RGPD secondo il quale *"I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.".*

Categorie di destinatari [17]. I dati sono comunicati:	☐ a struttura organizzativa competente per le attività di trattamento ☐ a struttura organizzativa diversa da quella competente per le attività di trattamento	*(inserire nominativi delle persone autorizzate [18])*
	Esternamente:	*(indicare quali)*
	☐ a soggetti diversi dal Consiglio regionale del Lazio	*(indicare quali)*
Periodo di conservazione dei dati personali[19]		

MODALITA' E STRUMENTI DI TRATTAMENTO

I dati sono elaborati e conservati su supporti cartacei	☐ sì ☐ no	*(indicare modalità di conservazione dei documenti e ubicazione)*
I dati sono elaborati e conservati mediante strumenti informatici	☐ mediante strumenti informatici "standard"	☐ cartelle su singole postazioni di lavoro ☐ cartelle di rete (su server) ☐ strumenti di elaborazione portatili (es., laptop/tablet…) ☐ strumenti di archiviazione remota (es., cloud) ☐ strumenti di archiviazione hw rimovibili (ad es., hd esterni, pen drive, cd-dvd rom…) ☐ _____ (*specificare*)
	☐ mediante sistemi informativi "comuni"	☐ posta elettronica ☐ posta elettronica certificata ☐ protocollo informatico ☐ _____ (*specificare*)
	☐ mediante sistemi informativi "verticali"[20]	*(indicare denominazione sistema informativo)*

17 Cfr. l'art. 4, n. 9 RGPD secondo il quale per "*destinatario*" si intende: "*la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento*".

18 Conformemente a quanto previsto dall'art. 411 bis, co. 3 del regolamento di organizzazione.

19 Ad es., facendo riferimento ad eventuali termini di legge o a regolamenti interni (ad es., massimario di scarto per categorie documentali); in assenza di indicazioni puntuali, indicare il periodo effettivo di conservazione ed i criteri utilizzati per determinarlo

20 Si fa riferimento a sw dedicati a specifiche funzionalità/attività/processi, quali ad es., il sw per l'elaborazione delle paghe, della contabilità, etc.

BANCHE DATI[21] ASSOCIATA AL TRATTAMENTO

Denominazione della banca dati	*(indicare la banca dati alla quale è associato il trattamento)*
Descrizione della banca dati	☐ cartacea ☐ elettronica ☐ mista
Ubicazione della banca dati *(rispetto alla struttura del CRL)*	☐ esterna ☐ interna
Sede della banca dati	……(*specificare*)
Amministratore di sistema che supporta la gestione della banca dati	……(*specificare*)
Responsabili del trattamento ex art. 28 RGPD che operano sulla banca dati	……(*specificare*)
Incaricati delle copie di sicurezza	……(*specificare*)
Persone autorizzate che possono operare sulla banca dati	……(*specificare*)

MISURE DI SICUREZZA ASSOCIATE ALLA BANCA DATI (ART. 32 GDPR) nota

Pseudonimizzazione[22]:	☐ presente ☐ non presente

21 Ai fini della compilazione del registro dei trattamenti per banca dati si intende una raccolta organizzata di dati interrelati memorizzata su un supporto e consultabili da parte di soggetti autorizzati. Tale raccolta di dati può essere gestita secondo qualunque modalità, non necessariamente automatizzata. Possono costituire banca dati, quindi: un archivio di fascicoli cartacei organizzato secondo criterio cronologico o alfabetico; un file MS Excel in cui viene memorizzata una lista di indirizzi e-mail di persone iscritte ad una newsletter o invitate ad un evento; un software (residente su un server del CRL ovvero su un cloud gestito da un soggetto terzo) in cui vengono memorizzati i dati personali necessari per la gestione di determinate pratiche, quali presenze, buste paga, ecc.

22 Cfr. l'art. 4, n. 5 RGPD secondo il quale per "*pseudonimizzazione*" si intende: *"il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione*

Cifratura dei dati personali[23]	☐ presente ☐ non presente
Accesso contemporaneo	☐ non consentito con la stessa credenziale di autorizzazione ☐ consentito con la stessa credenziale di autorizzazione
Password	☐ accesso all'archivio tramite password ☐ accesso all'archivio senza password
Cambio password	☐ possibilità autonoma di modifica ☐ possibilità non autonoma di modifica
Antintrusione	☐ è presente un programma di antintrusione: ..... (*specificare*) ☐ non è presente un programma di antintrusione
Controllo supporti	☐ i supporti non utilizzati vengono cancellati ☐ i supporti non utilizzati non vengono cancellati
Back–up	☐ periodicità di back-up: ..... (*specificare*) ☐ supporto di back-up: ..... (*specificare, ad esempio nastro magnetico ecc.*)
Descrizione di misure di sicurezza adottate[24]	..... (*specificare*)

ALTRE OPERAZIONI

I dati (ed i documenti in cui sono contenuti) dati sono soggetti a regime di pubblicità giuridica	☐ Pubblicità notizia ☐ Pubblicità integrativa dell'efficacia ☐ Pubblicità dichiarativa ☐ Pubblicità "trasparenza"
I dati sono oggetto di trasferimento in Paesi terzi (extra UE)	☐ sì ☐ no
I dati sono oggetto di trasferimento verso organizzazioni internazionali	☐ sì ☐ no

VALUTAZIONE PRELIMINARE D'IMPATTO

che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.".

23 Per *"cifratura"* si intende: *"il processo di conversione delle informazioni da un formato leggibile in un formato codificato, in modo da garantirne, rendendole incomprensibili a chiunque non sia autorizzato ad accedervi, la riservatezza/confidenzialità: solo chi possiede la chiave di lettura per decriptare il messaggio può così accedere alle informazioni nel formato originale. Gli elementi di tale processo sono: le informazioni da proteggere, l'algoritmo di cifratura o di criptaggio (ossia il software di cifratura/criptaggio dei dati), il crittogramma (testo cifrato) e un valore segreto definito chiave crittografica o di cifratura (password). Dato un crittogramma generato da un certo algoritmo di cifratura, il sistema non permette di risalire al testo in chiaro di un documento se non conoscendo la chiave di cifratura ossia la chiave usata per cifrare (criptare) il documento stesso.".*

24 Ad es., in caso di una banca dati cartacea si può indicare armadi chiusi a chiave, persone delegate alla custodia delle chiavi, in caso di una baca dati automatizzata si può indicare la presenza di antivirus, firewall, ecc.

La valutazione d'impatto sulla protezione dei dati personali o "DPIA" consiste in una procedura – da svolgere prima dell'avvio delle operazioni di trattamento sottoposte a valutazione – finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali.

Secondo quanto indicato dall'art. 35 RGPD, la DPIA è obbligatoria quando uno o più finalità di trattamento effettuati *"possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche".* Ed in particolare nei seguenti casi:

- una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- il trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati di cui all'art. 10 RGPD;
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Inoltre, le Linee Guida[25] adottate dal Working Party 29 identificano 9 criteri in presenza dei quali il trattamento potrebbe presentare un livello di "rischio inerente" potenzialmente elevato:

1. valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione[26];
2. processo decisionale automatizzato che ha effetti giuridici o incida in modo analogo significativamente sui diritti degli interessati[27];
3. monitoraggio sistematico, utilizzato per osservare, monitorare o controllare gli interessati ivi inclusi i dati raccolti tramite reti o *"la sorveglianza sistematica su larga scala di una zona accessibile al pubblico*"[28];
4. impedimento agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto[29];
5. creazione di corrispondenze, combinazione o messa in relazione di due o più insiemi di dati;
6. uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative[30];
7. dati sensibili o dati aventi carattere altamente personale ivi incluse le categorie particolari di dati personali così come definite all'articolo 9, GDPR, nonché dati personali relativi a condanne penali o reati di cui all'articolo 10, GDPR[31];

---

25 WP 248 rev. 01 Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del RGPD (rev. 04/10/2017), fatte proprie dal Comitato Europeo per la Protezione dei Dati il 25/05/2018

26 Ad es., secondo le Linee Guida citate "*un ente finanziario che esamina i suoi clienti rispetto a una banca dati di riferimento in materia di crediti oppure rispetto a una banca dati in materia di lotta contro il riciclaggio e il finanziamento del terrorismo (AML/CTF) oppure contenente informazioni sulle frodi; oppure un'impresa di biotecnologie che offre test genetici direttamente ai consumatori per valutare e prevedere i rischi di malattia o per la salute; oppure un'impresa che crea profili comportamentali o per la commercializzazione basati sull'utilizzo del proprio sito web o sulla navigazione sullo stesso*".

27 Ad es., il trattamento può portare all'esclusione o alla discriminazione nei confronti degli interessati. Laddove il trattamento abbia soltanto un effetto limitato sulle persone, potrebbe non rispondere al presente criterio.

28 In questo contesto, assumono particolare rilievo le circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come saranno trattati dal titolare ovvero sia impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico).

29 Il presente criterio include i trattamenti che sono finalizzati a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto.

30 Ad es., la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, l'implementazione di tecnologie IoT (Internet of Things), *etc*.

31 Inoltre, alcune categorie di dati possono far "aumentare" il possibile rischio per i diritti e le libertà delle persone fisiche. Tali dati personali sono considerati essere sensibili (nel senso in cui tale termine è comunemente compreso) perché sono legati ad attività a carattere personale o domestico (quali le comunicazioni elettroniche la cui riservatezza deve essere protetta) oppure perché influenzano l'esercizio di un diritto fondamentale (come ad esempio i dati relativi all'ubicazione, la cui raccolta mette in discussione la libertà di circolazione) oppure perché una eventuale violazione dei dati personali implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato (si pensi ad esempio a dati finanziari che potrebbero essere utilizzati per frodi relative ai pagamenti). A questo proposito, può essere rilevante il fatto che tali dati siano stati resi pubblici dall'interessato o da terzi. Il fatto che i dati personali siano di dominio pubblico può essere considerato un fattore da considerare nella valutazione qualora fosse previsto che i dati venissero utilizzati ulteriormente per determinate finalità. Inoltre, il presente criterio potrebbe ritenersi soddisfatto anche nel caso in cui i dati personali siano rappresentati da documenti personali, messaggi di posta elettronica, diari, note ricavate da dispositivi elettronici di lettura dotati di funzionalità di annotazione, nonché informazioni molto personali contenute nelle applicazioni che registrano le attività quotidiane delle persone.

8. trattamento di dati su larga scala[32];
9. dati relativi a interessati vulnerabili[33].

Le suddette Linee Guida dispongono che "*un trattamento che soddisfi due criteri debba formare oggetto di una valutazione d'impatto sulla protezione dei dati*".

Pertanto, coerentemente con tali principi, si richiede la compilazione della tabella di valutazione indicata qui di seguito. Qualora due o più criteri siano stati soddisfatti (risposta affermativa), sarà necessario valutarne il contenuto anche in funzione del Provvedimento dell'Autorità Garante n. 467 dell'11/10/2018[34] e assumere la decisione se svolgere una valutazione d'impatto sulla protezione dei dati personali.

Criterio	Valutazione (Sì/No)	Note
Assegnazione di un punteggio e/o profilazione		
Processo decisionale automatizzato		
Monitoraggio sistematico		
Impedimento agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto		
Combinazione di due o più insiemi di dati personali		
Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative		
Dati sensibili o aventi carattere altamente personale		

32 Posto che non vi è una definizione normativa del concetto di "larga scala", questo criterio deve essere valutato tenendo in considerazione quantomeno: *(i)* il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; *(ii)* il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; *(iii)* la durata, ovvero la persistenza, dell'attività di trattamento e *(iv)* la portata geografica dell'attività di trattamento;

33 Gli interessati vulnerabili possono includere i minori (i quali possono essere considerati non essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati), i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento.

34 Che ha definito un elenco delle tipologie di trattamento ai sensi dell'art. 35, par. 4 RGPD da sottoporre a valutazione d'impatto, redatta sulla base delle linee guida WP 248, rev. 01 ed allo scopo di specificarne ulteriormente il contenuto e a complemento delle stesse Linee guida.

Trattamento svolto su larga scala		
Dati personali riferibili a interessati vulnerabili		