REGIONE CALABRIA
GIUNTA REGIONALE

DIPARTIMENTO LAVORO, FORMAZIONE E POLITICHE SOCIALI (LFPS). SETTORE 05 -PARI OPPORTUNITA', POLITICHE DI GENERE, SERVIZIO CIVILE, IMMIGRAZIONE, CENTRO REGIONALE ANTIDISCRIMINAZIONE

Assunto il 01/10/2019

Numero Registro Dipartimento: 3287

DECRETO DIRIGENZIALE

“Registro dei decreti dei Dirigenti della Regione Calabria”

N°. *12227 del 09/10/2019*

OGGETTO: APPROVAZIONE DELLE VALUTAZIONI D'IMPATTO SULLA PROTEZIONE DEI DATI E DEI RELATIVI PIANI D'AZIONE EX ART. 35 REGOLAMENTO (UE) 2016/679.

Dichiarazione di conformità della copia informatica

Il presente documento, ai sensi dell’art. 23-bis del CAD e successive modificazioni è copia conforme informatica del provvedimento originale in formato elettronico, firmato digitalmente, conservato in banca dati della Regione Calabria.

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

IL DIRIGENTE GENERALE

VISTI/E:

- La legge regionale 13 maggio 1996, n. 7, recante “Norme sull’ordinamento della struttura organizzativa della Giunta Regionale e sulla Dirigenza Regionale” ed in particolare l'art. 28 che individua i compiti e le responsabilità del Dirigente con funzioni di Dirigente Generale;
- Il D.P.G.R. n. 354 del 24 giugno 1999,recante norme sulla “separazione dell’attività amministrativa di indirizzo e controllo da quella di gestione”, modificato con D.P.G.R. nr. 206 del 15 dicembre 2000;
- La D.G.R. n. 468 del 19 ottobre 2017 con la quale, tra l’altro, si è disposto di scorporare il Dipartimento “Sviluppo Economico, Lavoro, Formazione e Politiche Sociali” in due Dipartimenti corrispondenti alle due aree funzionali preesistenti, ovvero “Lavoro, Formazione e Politiche Sociali” e “Sviluppo Economico – Attività Produttive”;
- La D.G.R. n. 63 del 15/02/2019 “Struttura organizzativa della Giunta Regionale – Approvazione. Revoca della struttura organizzativa approvata con D.G.R. nr. 541/2015 e s.m.i.;
- La D.G.R. n. 241 ad oggetto: “Struttura organizzativa della Giunta regionale. Approvazione modifiche della delibera di Giunta regionale n. 63 del 15/02/2019”;
- La D.G.R. nr. 186 del 21/05/2019 “DGR nr. 63 del 15/02/2019: struttura organizzativa della Giunta Regionale - Approvazione revoca della struttura organizzativa approvata con DGR nr. 541/2015 e s.m.i.- Pesatura delle posizioni dirigenziali e determinazione delle relative fasce di rischio”;
- La D.G.R. n. 228 del 06/06/2019 con la quale il Dott. Roberto Cosentino è stato individuato quale Dirigente Generale Reggente del Dipartimento Lavoro, Formazione e Politiche Sociali;
- Il D.P.G.R. n. 76 del 10 giugno 2019 con il quale il Dott. Roberto Cosentino è stato nominato Dirigente Generale Reggente del Dipartimento Lavoro, Formazione e Politiche Sociali;
- Il D.D.G. n. 6699 del 05/06/2019 con il quale è stato conferito alla dott.ssa Edith Macrì, l’incarico di dirigente temporaneo reggente del Settore n.5 “Pari opportunità, Politiche di genere, Servizio civile, Immigrazione e Centro Regionale Antidiscriminazioni” del Dipartimento “Lavoro, Formazione e Politiche Sociali” e in attuazione della DGR nr. 186/2019;
- La D.G.R. n. 36 del 30.01.2019 “Approvazione Piano Triennale della Prevenzione della Corruzione e della trasparenza 2019/2021. Aggiornamento 2019”;

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);

VISTO l’articolo 35 del GDPR 2016/679 che:

- Al paragrafo 1 prevede che: ”*Quando un tipo di trattamento, allorchè prevede in particolare l’uso di nuove tecnologie, considerati la natura, l’oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione d’impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi”.*
- Al paragrafo 2 prevede che: ”*Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno”.*
- Al paragrafo 3 prevede che*: “la valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti: a)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; b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o c) la sorveglianza sistematica su larga scala di una zona accessibile*

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

al pubblico".

- Al paragrafo 7 prevede che: *"La valutazione contiene almeno: a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione".*
- Al paragrafo 9 prevede che*:"Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti".*

CONSIDERATO CHE:

- la valutazione di impatto compete ai titolari, con il responsabile della protezione dei dati cui viene chiesto apposito parere, e ai responsabili del trattamento;
- Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.
- Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.
- Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.
- Per la redazione delle Valutazioni di impatto è stato utilizzato il software PIA, redatto dal Garante francese e posto a disposizione in versione italiana sul sito del Garante Italiano;
- Con la Delibera 11 ottobre 2018, n. 467 del Garante per la protezione dei dati personali sono state elencate le tipologie di trattamenti, ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679, da sottoporre a valutazione di impatto sulla base dei seguenti criteri:
    1. valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato";
    2. processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente sulle persone;
    3. monitoraggio sistematico degli interessati;
    4. dati sensibili o dati aventi carattere altamente personale;
    5. trattamento di dati su larga scala;
    6. creazione di corrispondenze o combinazione di insiemi di dati;
    7. dati relativi a interessati vulnerabili;
    8. uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative;
    9. quando il trattamento in se' impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto;

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Con specifico riferimento al settore, i procedimenti per i quali è richiesta una valutazione di impatto, in quanto vengono trattati anche dati sensibili, dati giudiziari e dati aventi carattere altamente personale, sono i seguenti:

1) Prevenzione e contrasto violenza sulle donne;
2) Protezione Dati destinatari Corsi di Alfabetizzazione Progetto Calabria Friends - Fondo Asilo Migrazione e Integrazione 2014-2020 e degli Ospiti per il progetto INCIPIT;
3) Protezione Dati Casellario Giudiziale Dipendenti.

DATO ATTO che:

- Con nota n. 323063 del 18/09/2019 lo scrivente Settore ha chiesto al DPO della Regione Calabria, Avv. Angela Stellato, il parere in merito alla valutazione di impatto redatta da questo Settore in materia di Prevenzione e contrasto violenza sulle donne e che quest'ultimo ha espresso parere positivo con nota n. 329024 del 23/09/2019;

- Con nota n. 325289 del 19/09/2019 lo scrivente Settore ha chiesto al DPO della Regione Calabria, Avv. Angela Stellato , il parere in merito alla valutazione di impatto redatta da questo Settore in materia di Protezione Dati Casellario Giudiziale Dipendenti e che quest'ultimo ha espresso parere positivo con nota n. 329046 del 23/09/2019;

- Con nota n 331430 del 25/09/2019 lo scrivente Settore ha chiesto al DPO della Regione Calabria, Avv. Angela Stellato, il parere in merito alla valutazione di impatto redatta da questo Settore in materia di Protezione Dati destinatari Corsi di Alfabetizzazione Progetto Calabria Friends - Fondo Asilo Migrazione e Integrazione 2014-2020 e degli Ospiti per il progetto INCIPIT e che quest'ultimo ha espresso parere positivo con nota n. 335014 del 27/09/2019;

RITENUTO OPPORTUNO approvare le Valutazioni d'Impatto e i relativi Piani d'azione allegati al presente atto a costituirne parte integrante e sostanziale, per come redatti dal settore adoperando il software messo a disposizione del Garante;

CONSIDERATO che il presente atto non produce effetti di spesa;

RITENUTA la propria competenza ed attestata, sulla scorta dell'istruttoria effettuata, la regolarità amministrativa nonché la legittimità e correttezza del presente atto.

VISTI/E, altresì:

- La legge n. 241 del 07/08/1990 recante "*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*", coordinato ed aggiornato da ultimo, dal d.lgs. nr. 127 del 30.06.2016, dal d.lgs. 222 del 25/11/2016 e dal d.lgs. nr. 104 del 16.06.2017.
- Il D.lgs. nr. 196 del 30.06.2003 "*Codice in materia di protezione dei dati personali*" e ss.mm.ii;
- 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);
- Il D.P.R. n. 445 del 28/12/2000 "*Testo Unico sulla documentazione amministrativa*";
- la Legge Regionale n. 34/2002 recante "*Riordino delle funzioni amministrative regionali e locali*" e s.m.i., per la quale viene ritenuta la propria competenza;

SU proposta del funzionario responsabile del procedimento formulata alla luce dell'istruttoria compiuta che ne ha riscontrato la regolarità tecnico-amministrativa;

DECRETA

Per le motivazioni espresse in narrativa che qui si intendono integralmente ripetute e confermate per costituirne parte integrante e sostanziale del presente provvedimento:

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

DI approvare le Valutazioni di Impatto e i relativi Piani d'Azione allegati al presente atto a costituirne parte integrante e sostanziale, per come redatti dal settore adoperando il software messo a disposizione del Garante del trattamento dei dati personali relativi ai procedimenti sotto indicati:

1.Prevenzione e contrasto violenza sulle donne;

2.Protezione Dati destinatari Corsi di Alfabetizzazione Progetto Calabria Friends - Fondo Asilo Migrazione e Integrazione 2014-2020 e degli Ospiti per il progetto INCIPIT;

3.Protezione Dati Casellario Giudiziale Dipendenti.

DI dare atto che le misure individuate a tutela dei dati saranno oggetto di riesame e aggiornamento, qualora necessario;

Di notificare il presente decreto al Presidente della Giunta Regionale, al Dirigente del settore "Datore di Lavoro, sicurezza luoghi lavoro,privacy e al DPO;

Di invitare i dipendenti autorizzati al trattamento dei dati al rispetto delle prescrizioni di legge, nonché delle previsioni contenute nelle valutazioni allegate al presente atto;

DI disporre la pubblicazione del presente provvedimento e delle allegate valutazioni di impatto sul Bollettino della Regione Calabria ai sensi della L.R. 11/2011 a cura del responsabile dipartimentale per la pubblicazione e sul sito Istituzionale della Regione.

Sottoscritta dal Responsabile del Procedimento
PARENTE ANGELO
(con firma digitale)

Sottoscritta dal Dirigente
MACRI' EDITH
(con firma digitale)

Sottoscritta dal Dirigente Generale
COSENTINO ROBERTO
(con firma digitale)

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Informazioni sulla PIA

Nome della PIA **Prevenzione e contrasto violenza sulle donne**

Nome autore	Angelo Parente

Nome valutatore	Edith Macrì

Nome validatore	Roberto Cosentino

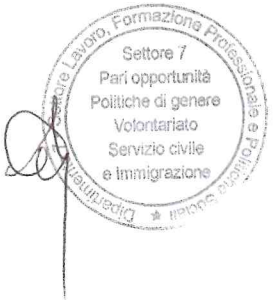
Data creazione	17/09 /2019

Nome del DPO/RPD	Angela Stellato

Parere del DPO/RPD	Positivo (nota n. 329024 del 23/09/2019)

Richiesta del parere degli interessati Non è stato chiesto il parere degli interessati

Motivazione della mancata richiesta del parere degli interessati La platea degli interessati non è predeterminabile e individuabile a priori. Non è dunque possibile individuare preventivamente degli interessati



Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Contesto

Panoramica del trattamento

Qual è il trattamento in considerazione?

Gestione dati personali e sensibili delle donne vittime di violenza e loro figli nonché di minori vittime di violenza domestica diretta o assistita, presi in carico dai Centri antiviolenza e dalle Case rifugio autorizzati al funzionamento e destinatari di contributi finanziari pubblici, soggetti in conseguenza di ciò a controllo.

Quali sono le responsabilità connesse al trattamento?

Il responsabile di procedimento e i collaboratori interni ed esterni assumono cognizione dei dati personali delle utenti e dei loro figli minori, in condizioni di disagio a seguito di violenze, abusi e maltrattamenti subiti, bisognevoli, oltre che di assistenza, di protezione e sicurezza e, nei casi più gravi, ospitati presso strutture protette a indirizzo segreto. I dati sono normalmente annotati, a mezzo di apposito codice criptato, in appositi registri presso i Centri e tenuti in armadi chiusi a chiave. Tali registri sono trasmessi alla Regione ai fini del controllo sui servizi erogati e per i quali la stessa eroga contributi pubblici.

Pertanto i dati personali di tali soggetti, contenuti in detti registri anche se in forma criptata e inviati agli uffici regionali, devono essere accuratamente trattati e conservati onde evitare indebiti accessi dall'esterno.

Ci sono standard applicabili al trattamento?

Il responsabile di procedimento è tenuto a garantire, unitamente ai propri collaboratori interni ed esterni, la riservatezza dei dati curando la conservazione delle pratiche cartacee e, in particolare, adottando particolari cautele nella gestione dei sistemi informatici. E' stata prevista la codifica del dato da parte di ciascun Centro antiviolenza in modo da tutelarne la riservatezza.

Valutazione: Migliorabile

Piano d'azione – misure correttive

E' prevista l'applicazione di un protocollo standard per la codifica/decodifica del dato da applicare uniformemente sul territorio da ogni Centro antiviolenza e ogni Casa Rifugio e in futuro ad ogni servizio di accoglienza, supporto, assistenza, ospitalità finanziato dalla Regione

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Dati personali quali Cognome Nome, data di nascita, Codice Fiscale, Indirizzo di residenza. I dati sono raccolti a fini statistici e di programmazione dei servizi in quanto richiesti da ISTAT, Dipartimento delle Pari Opportunità e Regione Calabria.

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

Dipartimento Lavoro, Formazione Professionale e Politiche Sociali
Settore 6
Pari opportunità
Politiche di genere
Volontariato
Servizio civile
e Immigrazione

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

I registri, contenenti già dati codificati, sono inviati a mezzo pec su file protetti da password. La password di accesso al file è poi inviata separatamente sulla e-mail istituzionale del responsabile del procedimento. I registri riportano per ogni utente solo un codice criptato i cui parametri di decriptazione sono standardizzati. Tale doppio canale mira a garantire sufficientemente l'accesso accidentale o non autorizzato ai registri e ai dati personali e sensibili delle titolari. **Quali sono le risorse di supporto ai dati?** Una volta acquisiti, i registri sono memorizzati su supporti esterni (CD_ROM-hard disk), se pervenuti via pec queste sono cancellate onde evitare ricostruzioni o futuri accessi ai dati. I supporti esterni (CD-ROM, Hard disk) sono custoditi dal Responsabile di Procedimento
Valutazione: Accettabile

Settore 6
Pari opportunità
Politiche di genere
~~Volontariato~~
Servizio civile
e Immigrazione

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Principi fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi? Il trattamento dei dati risulta necessario al fine di consentire all'Ente regionale, a seguito dell'erogazione di fondi pubblici, di effettuare il prescritto controllo amministrativo contabile, non solo in relazione ai presupposti che giustificano le somme erogate ma anche onde evitare duplicazione di pagamenti e quindi favorire una sana gestione della spesa pubblica
Valutazione: Accettabile

Quali sono le basi legali che rendono lecito il trattamento? Richiesto dalle disposizioni vigenti (L.328/2000, L.R.23/2003, L.R. 20/2007, Legge 119/2013, Intesa Stato Regioni 27/11/2014 - DGR 539/2017- DPCM 25/11/2016 – DPCM 1.12.2017 e seguenti)
Valutazione: Accettabile

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)? Non sono richiesti dati ulteriori a quelli necessari per il controllo ammistrativo-contabile a giustificazione delle spese sostenute e cioè relativamente ai dati anagrafici e fiscali (Cognome e nome, data di nascita, residenza e codice fiscale).
Valutazione: Accettabile

I dati sono esatti e aggiornati? I dati sono forniti dai Centri antiviolenza e dalle Strutture di accoglienza delle donne vittime di violenza e loro figli mediate l'invio di copia dei registri criptati, crittografati e protetti da password. Essi sono riferiti all'arco temporale coperto dal contributo pubblico.
Valutazione: Accettabile

Qual è il periodo di conservazione dei dati?

Dipartimento Lavoro, Formazione Professionale e Politiche Sociali
Settore 5
Pari opportunità
Politiche di genere
Volontariato
Servizio civile
e Immigrazione

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Il periodo di conservazione dei dati è legato ai possibili controlli da parte degli organi a ciò deputati per cui è di non meno di cinque anni
Valutazione: Accettabile

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati? All'atto della presa in carico il centro o la struttura antiviolenza sottopone una nota informativa.
Valutazione: Migliorabile **Piano d'azione / misure correttive:** Prevedere una informativa web più ampia e descrittiva da inviare anche ai Centri e alle strutture di accoglienza delle donne vittime di violenza e loro figli in modo da uniformare il format in tutti i Centri antiviolenza e nelle Case Rifugio. Detto format andrà pubblicato sul sito web regionale corredato da apposita nota informativa

Ove applicabile? Come si ottiene il consenso degli interessati? All'atto della presa in carico presso i Centri antiviolenza e le Case Rifugio
Valutazione: Accettabile

Come fanno gli interessati ad esercitare i loro diritti di accesso e di portabilità dei dati? Inviando una mail al Centro antiviolenza/Casa Rifugio e alla Regione Calabria
Valutazione: Accettabile

Come fanno gli interessati ad esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)? Inviando una mail al Centro antiviolenza/Casa Rifugio e alla Regione Calabria
Valutazione: Accettabile

Dipartimento Lavoro, Formazione Professionale e Politiche Sociali
Settore 6
Pari opportunità
Politiche di genere
Volontariato
Servizio civile
e Immigrazione

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Come fanno gli interessati ad esercitare i loro diritti di limitazione e opposizione? Inviando una mail al Centro antiviolenza/Casa Rifugio e alla Regione Calabria
Valutazione: Accettabile

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto? Obblighi a trattare i dati garantendo riservatezza sono imposti apposita nota di nomina la cui violazione può comportare l'applicazione di sanzioni disciplinari
Valutazione: Accettabile

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di protezione equivalente Non è previsto il trasferimento dei dati al di fuori dell'UE
Valutazione: Accettabile

Come sono informati del trattamento gli interessati?
Valutazione: Accettabile

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Rischi

Misure esistenti o pianificate

Accesso riservato da password

I dati contenuto nei registri detenuti dai Centri Antiviolenza/Case Rifugio sono annotati sotto forma di codice criptato. Detti registri sono inviati tramite pec alla pec istituzionale del Settore regionale mediante file protetti da password e acquisiti ufficialmente al protocollo generale. La password per l'accesso a detti file e poi inviata separatamente alla casella e-mail istituzionale personale del Responsabile del Procedimento. Sia la pec del settore sia la mail istituzionali sono protette da password. L'accesso ai Computer dell'addetto alla gestione delle pec e del Responsabile del procedimento è protetto da password. Il file ricevuto a mezzo pec è inoltrato al Responsabile del Procedimento e, per conoscenza, al Dirigente del Settore (che comunque ha già accesso diretto alla pec).

Valutazione: Accettabile

Limitazione della permanenza dei file di dati sul server

Una volta protocollato il messaggio di trasmissione via pec del file criptato e protetto da password, lo stesso ed il relativo allegato è cancellato per cui tali informazioni sono detenute sul server di ARUBA solo per il tempo necessario all'acquisizione formale al protocollo generale dell'ente regionale ed allo smistamento.

Dopo essere stati formalmente acquisiti, i registri sono scaricati e memorizzati su supporti esterni (CD_ROM-hard disk), e le e-mail di ricezione e rispettivi allegati sono cancellati. I supporti esterni (CD-ROM, Hard disk) e le stampe delle password sono custoditi dal Responsabile di Procedimento in appositi contenitori/plichi/buste chiusi e sigillati sui lembi con firma dal RUP. Gli stessi sono custoditi in armadi chiusi a chiave.

Se utilizzati dal Responsabile del procedimento per ragioni di controllo amministrativo/contabile devono essere richiusi e sigillati con le stesse modalità, annotando all'interno la data dell'ultimo utilizzo.

Valutazione: Accettabile

Accesso illegittimo ai dati

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

Tutti i Dati riguardanti le donne prese in carico dai Centri antiviolenza e dalle Case rifugio, compresi quelli anagrafici, ed i loro figli sono da ritenersi sensibili e vanno

Settore 5
Pari opportunità
Politiche di genere
Volontariato
Servizio civile
e Immigrazione

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

assolutamente protetti in quanto ogni elemento atto a identificarne la persona titolare può metterne in pericolo la loro stessa incolumità. Attraverso accessi non autorizzati e abusivi dei dati l'uomo maltrattante, o anche membri della sua famiglia o conoscenti, potrebbero scoprire che la donna si è rivolta ai servizi antiviolenza e per questo attuare forme di ritorsione, inasprimento di violenze, scoprire dove la stessa si è rifugiata ed attuare anche gesti estremi, come i fatti di cronaca purtroppo testimoniano. Per tale motivo le Case rifugio sono a indirizzo segreto.

Quali sono le principali minacce che potrebbero concretizzare i rischio?

Conoscenza dei dati da accesso abusivo al sistema informatico esterno ARUBA/Pec organizer;

Conoscenza dei dati da accesso abusivo ai computer in dotazione al Settore;

Quali sono le fonti di rischio?

Soggetti esterni all'amministrazione che accedono abusivamente al sistema ARUBA PEC, soggetti esterni all'amministrazione che apprendano copie delle pratiche cartacee in lavorazione. Soggetti interni all'amministrazione che accedono ai computer in dotazione e ai supporti informatici di archiviazione.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Limitazione della permanenza dei dati(file) sul server di ARUBA/Pec organizer e sulle e-mail istituzionali personali;

Accessi riservati da password, ai file e alle macchine.

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

Importante. I dati personali e sensibili delle donne vittime di violenza e loro figli se posti a conoscenza di terzi possono comportare gravi conseguenze per la sicurezza e la dignità dei titolari di tali dati.

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

Trascurabile: I dati sono codificati nei registri, acquisiti a mezzo file protetti da password, conservati su supporti informatici protetti e custoditi in contenitori sigillati e chiusi in armadi, cancellati dai server di ARUBA/Pec organizer.

Valutazione: Migliorabile

Settore 5
Pari opportunità
Politiche di genere
Volontariato
Servizio civile
e Immigrazione

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Piano d'azione /misure correttive

- Modificare con media frequenza le credenziali di accesso su server esterno PEC ARUBA/Organizer da parte degli operatori, al fine di evitare il permanere della conoscenza di tali credenziali nell'ipotesi di cessazione delle relative mansioni;

Alla luce del Piano d'azione, come valutate *la gravità di questo rischio* (Accesso illegittimo ai dati)? Trascurabile;

Alla luce del Piano d'azione, come valutate *la probabilità di questo rischio* (Accesso illegittimo ai dati)? Trascurabile;

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Per le utenti non se ne ravvedono. Per la pubblicazione amministrazione si può ipotizzare l'impossibilità ad effettuare i dovuti controlli.

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

La modificazione accidentale o dolosa dei dati è improbabile. I dati sono conservati in formato pdf immodificabile.

Valutazione: Migliorabile

Piano d'azione / misure correttive

Prevedere il back up dei dati in modo da duplicare la conservazione. I file copiati saranno conservati a cura del Responsabile del procedimento e del Dirigente

Quali sono le fonti di rischio?

Non se ne ravvedono

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

Codifica dei dati, Accesso riservato con password, custodia in sicurezza, file pdf immodificabili, back up dei dati.

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

Trascurabile per le utenti non avrebbero alcuna conseguenza dalla modificazione

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

del dato.

Importante per la pubblica amministrazione compromettendone le possibilità del controllo amministrativo contabile in relazione ai servizi finanziati con fondi pubblici

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

Trascurabile. Il rischio di modifica dei dati è altamente improbabile alla luce delle misure previste.

Valutazione: Migliorabile

Piano d'azione / misure correttive

Effettuare confronti a campione tra i file originali e i file di back up al fine di verificare eventuali modificazioni.

Alla luce del Piano d'azione, come valutate *la gravità di questo rischio* (Modifiche indesiderate dei dati)? Trascurabile;

Alla luce del Piano d'azione, come valutate *la probabilità di questo rischio* (Modifiche indesiderate dei dati)? Trascurabile;

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?
Non se ne ravvedono. La PA potrebbe invece dovere giustificare concessioni di benefici non riscontrabili
Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?
Problemi tecnici sul server PEC ARUBA, accessi indesiderati sui server, rottura macchine e supporti informatici di archiviazione
Quali sono le fonti del rischio?
Hackeraggio e obsolescenza, senescenza e guasto hadware.
Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?
Ridondanza nella trasmissione dei file pervenuti (al RUP e al Dirigente), back up di sicurezza, accesso ai file e alle pec riservato da password
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?
Trascurabile per le utenti (donne vittime di violenza) e loro figli.
Importante per la PA che potrebbe non assolvere ai doveri di controllo e non poter verificare la legittimità dei benefici erogati
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?
Trascurabile.

Valutazione: Accettabile

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Piano d'azione

Panoramica

Panoramica del Trattamento
Principi fondamentali
Finalità
Basi legali
Adeguatezza dei dati
informativa
Esattezza dei dati
Periodo di conservazione
Misure a tutela dei diritti degli interessati
Informativa
Raccolta del consenso
Diritto di rettifica e diritto di cancellazione
Diritto di limitazione e di opposizione
Responsabili del trattamento

Misure esistenti
Accesso riservato da password
Limitazione alla permanenza dei dati su server esterni

Rischi
Accesso illegittimo ai dati
Modifiche indesiderate dei dati

Misure Migliorabili
Misure Accettabili

Contesto

Panoramica del trattamento

Piano d'azione / misure correttive:
E' prevista l'applicazione di un protocollo standard per la codifica/decodifica del dato da applicare uniformemente sul territorio da ogni Centro antiviolenza e ogni Casa Rifugio e in futuro ad ogni servizio di accoglienza, supporto, assistenza, ospitalità finanziato dalla Regione.

Data prevista implementazione: 31/12/2019
Responsabile dell'implementazione: Dirigente Settore Pari Opportunità/Responsabile del Procedimento

Principi fondamentali

Informativa

Piano d'azione / misure correttive:
Prevedere una informativa web più ampia e descrittiva da inviare anche ai Centri e alle strutture di accoglienza delle donne vittime di violenza e loro figli in modo da uniformare il format in tutti i Centri antiviolenza e nelle Case Rifugio. Detto format andrà pubblicato sul sito web regionale corredato da apposita nota informativa.

Data prevista implementazione: 31/12/2019
Responsabile dell'implementazione: Dirigente Settore Pari Opportunità/Responsabile del Procedimento

Settore 5 Pari opportunità politiche di genere servizio civile e immigrazione

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Rischi

Accesso illegittimo ai dati

Piano d'azione / misure correttive:

Modificare con media frequenza le credenziali di accesso su server esterno PEC ARUBA da parte degli operatori, al fine di evitare il permanere della conoscenza di tali credenziali nell'ipotesi di cessazione delle relative mansioni;

Data prevista implementazione: 31/12/2019
Responsabile dell'implementazione: dipendenti/ Dirigente Settore Pari Opportunità

Alla luce del piano d'azione, come valutate la gravità di questo rischio (Accesso illegittimo ai dati)? **Trascurabile**
Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Accesso illegittimo ai dati)? **Trascurabile**

Modifiche indesiderate dei dati

Piano d'azione / misure correttive:

Effettuare confronti a campione tra i file contenuti nei diversi archivi di back up, al fine di verificare eventuali modificazioni

Data prevista implementazione: 31/12/2019
Responsabile dell'implementazione: Responsabile del procedimento

Alla luce del piano d'azione, come valutate la gravità di questo rischio (Modifiche indesiderate dei dati)? **Trascurabile**
Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Modifiche indesiderate dei dati)? **Trascurabile**

Perdita dei dati

Piano d'azione / misure correttive:

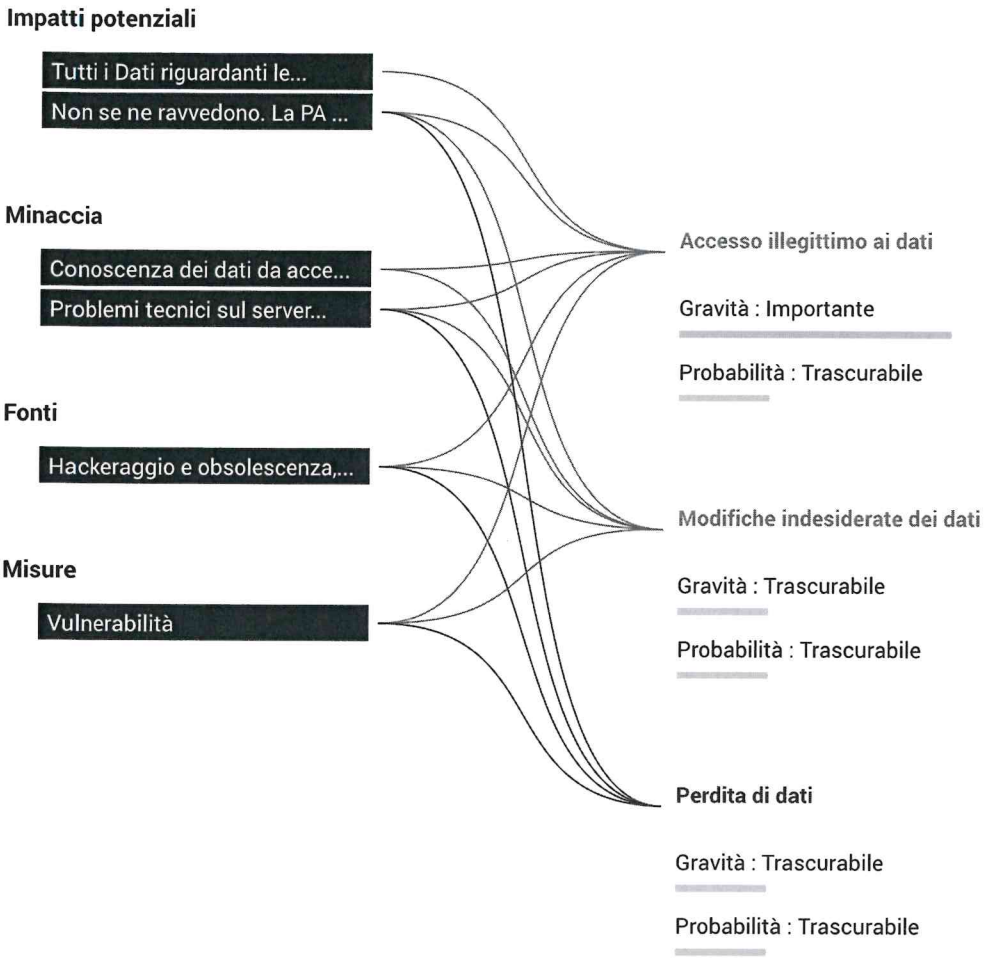
- Prevedere il back up dei dati in modo da duplicare la conservazione. I file copiati saranno conservati a cura del Responsabile del procedimento e del Dirigente

- Effettuare confronti a campione tra i file originali e i file di back up al fine di verificare eventuali modificazioni.

Data prevista implementazione: 31/12/2019
Responsabile dell'implementazione: Responsabile del Procedimento
Alla luce del piano d'azione, come valutate la gravità di questo rischio (Perdita dei dati)?
Trascurabile
Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Perdita dei dati)?
Trascurabile

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Panoramica dei rischi

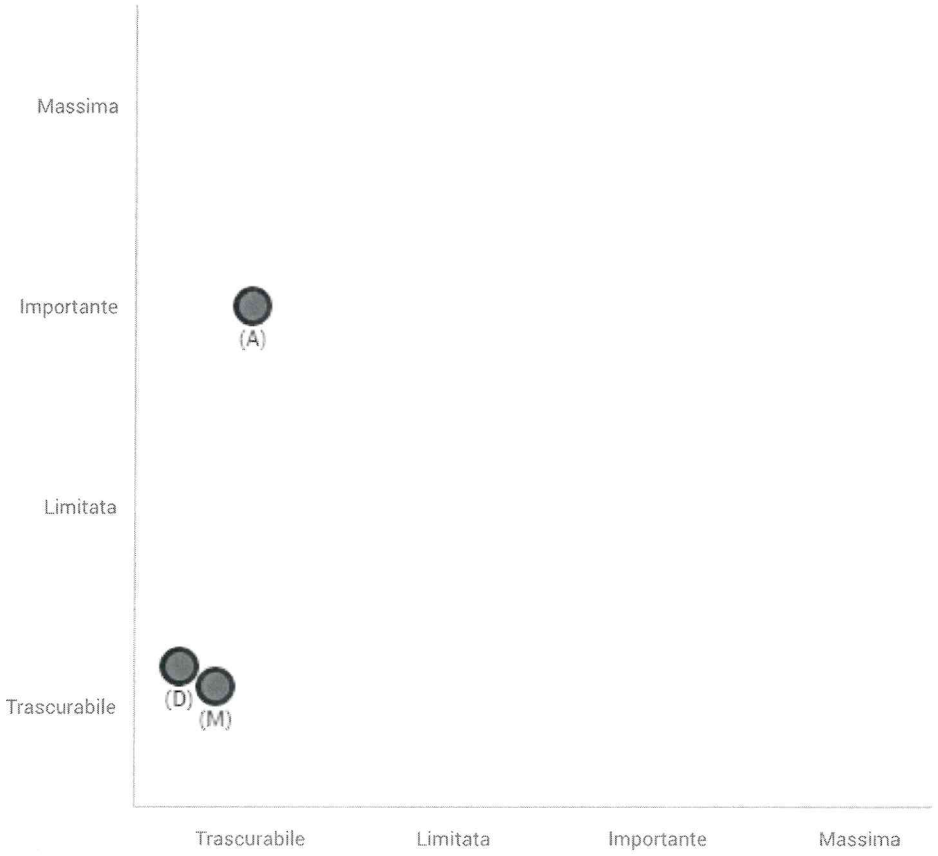


Settore 5
Pari opportunità
Politiche di genere
Volontariato
Servizio civile
e Immigrazione

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Mappaggio dei rischi

Gravità del rischio



Probabilità del rischio

- Misure pianificate o esistenti
- **Con le misure correttive implementate**
- **(A)ccesso illegittimo ai dati**
- **(M)odifiche indesiderate dei dati**
- **(P)erdita di dati**

28/08/2019

Settore 6
Pari opportunità
Politiche di genere
Volontariato
Servizio civile
e Immigrazione

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Informazioni sulla PIA

Nome della PIA Protezione Dati Casellario Giudiziale Dipendenti	
Nome autore	Angelo Parente
Nome valutatore	Edith Macrì
Nome validatore	Roberto Cosentino
Data creazione	17/09/2019
Nome del DPO/RPD	Angela Stellato
Parere del DPO/RPD	POSITIVO (nota 329046 del 23/09/2019)
Richiesta del parere degli interessati E' stato chiesto il consenso degli interessati. Consenso espresso al trattamento ed alla comunicazione dei propri dati personali forniti, con particolare riferimento a quelli sensibili e giudiziari.	
Motivazione della mancata richiesta del parere degli interessati	

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Contesto

Panoramica del trattamento

Qual è il trattamento in considerazione?

Gestione dati personali forniti dai dipendenti e collaboratori, con particolare riferimento a quelli definiti particolari e giudiziari, di cui al Regolamento UE n. 2016/679 e al D.lgs. 196/2003, presi in carico dal settore ai fini delle verifiche richieste circa l'insussistenza di condanne per i reati previsti nel capo I del titolo II del libro secondo del codice penale. Cio in quanto trattasi di misura di prevenzione della corruzione nella formazione di commissioni, assegnazione agli uffici e conferimento di incarichi, secondo le modalità previste nel Piano Triennale per la Prevenzione della Corruzione e la Trasparenza 2019/2021 di cui alla D.G.R. nr. 36/2019. I dati sono stati acquisiti ai fini del controllo anche a campione delle dichiarazioni rese.

Quali sono le responsabilità connesse al trattamento?

Il personale a ciò deputato, assume cognizione dei dati giudiziari, dei dipendenti e collaboratori, sottoposti a verifica delle autocertificazioni. I dati relativi a condanne penali e a reati previsti nel capo I del titolo II del libro secondo del codice penale, o l'assenza delle stesse sono trasmessi via Pec al settore, da parte del Casellario giudiziale competente in riscontro alla richiesta di verifica. L'eventuale assenza o presenza di condanne iscritte sul Casellario Giudiziale, deve essere comunicata al Dirigente per le conseguenti misure da applicare. I dati giudiziari, trasmessi al settore, devono essere accuratamente trattati e conservati onde evitare indebiti accessi dall'esterno e da parte di soggetti non deputati a farlo.

Ci sono standard applicabili al trattamento?

Il personale è tenuto a garantire, la riservatezza dei dati, curando la conservazione delle pratiche cartacee e, in particolare, adottando particolari cautele nella gestione dei sistemi informatici. In particolare deve annotare il protocollo in entrata in modalità riservato, in modo da non essere rintracciabile con semplice ricerca diretta. Le pratiche cartacee devono essere conservate in appositi fascicoli ed armadi chiusi a chiave. I file sono custoditi dal personale autorizzato e non inoltrati per conoscenza su altre mail - PEC.

Valutazione: Migliorabile

Piano d'azione – misure correttive

Particolari cautele devono essere adottate in riferimento al trattamento del dato giudiziario che può presentare un rischio elevato per i diritti e le libertà della persona fisica. Tenendo conto che non sembra sufficiente informare il dipendente della misura di controllo e acquisirne il relativo consenso, si ritiene utile provvedere alla conservazione dei dati su appositi supporti esterni (CD-rom- Hard Disk) custoditi dal personale autorizzato. Il responsabile del procedimento adotta

Settore 5 Pari opportunità Politiche di genere Servizio civile e Immigrazione

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

opportune misure atte al rispetto della norma a salvaguardia dell'accesso accidentale ovvero non autorizzato. In particolare il RUP si attiene a tutte le disposizioni regionali sulla sicurezza dei dati, anche secondo le disposizioni regionali vigenti. Nella richiesta di dati giudiziari il RUP circoscrive la richiesta ai soli dati necessari relativi ad eventuali reati previsti nel capo I, del titolo II, del libro secondo del codice penale.

Dati, processi e risorse di supporto

Quali sono i dati trattati?
Dati personali quali Cognome, Nome, data di nascita, luogo di nascita, Codice Fiscale, Indirizzo di residenza, dato giudiziario acquisito dal Casellario Giudiziale.
Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?
I dati personali dei dipendenti vengono acquisiti ai fini della richiesta di verifica al Casellario Giudiziale competente. Il riscontro viene acquisito tramite Pec e protocollato in modalità riservata. Viene conservato in modalità cartacea in busta chiusa, firmata e timbrata sui lembi, tenuta in appositi fascicoli all'interno di armadi chiusi a chiave, a cura del personale autorizzato.
Quali sono le risorse di supporto ai dati?
Una volta acquisiti, i dati sono stampati e conservati in appositi fascicoli riposti in armadi chiusi a chiave, in busta chiusa, firmata e timbrata sui lembi, insieme alle risultanze della verifica. I file di quest'ultima, permangono sulla Pec di ricezione e sul sistema di protocollazione dell'Ente.

Valutazione: Accettabile

Dipartimento Settore Lavoro, Formazione Professionale e Politiche Sociali
Settore 5
Pari opportunità
Politiche di genere
~~Volontariato~~
Servizio civile
e Immigrazione

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Principi fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi? Il trattamento dei dati risulta necessario al fine di consentire all'Ente regionale, di effettuare i controlli in merito al rispetto della misura di prevenzione della corruzione nella formazione di commissioni, assegnazione agli uffici e conferimento di incarichi, secondo le modalità previste nel Piano Triennale per la Prevenzione della Corruzione e la Trasparenza 2019/2021 di cui alla D.G.R. nr. 36/2019.
Valutazione: Accettabile

Quali sono le basi legali che rendono lecito il trattamento? Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza è considerato lecito sulla base dell'articolo 6, lett.a) ed e) paragrafo 1, del GPDR 679/2016 e deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri prevedere garanzie appropriate per i diritti e le libertà degli interessati. Inoltre la base normativa legittimante il trattamento dei dati giudiziari si rinviene nei seguenti atti e riferimenti legislativi: - Art. 35 bis del D.lgs n.165/2001 - CCNL comparto EE.LL. - Codice comportamento dei dipendenti della Regione Calabria (DGR n.25 del 31/01/2018) - Piano Triennale per la Prevenzione della Corruzione e la Trasparenza 2019/2021 di cui alla D.G.R. nr. 36/2019;
Valutazione: Accettabile

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)? Non sono forniti dati ulteriori a quelli necessari per la verifica al Casellario Giudiziale e cioè: dati anagrafici e fiscali (Cognome e nome, data di nascita, luogo di nascita, residenza, codice fiscale). Allo stesso modo sono richiesti i dati giudiziari strettamente correlati al procedimento amministrativo in corso, in particolare limitatamente a quelli strettamente necessari alla verifica di cui all'art.35 bis del D.lgs n.165/2001, come in precedenza evidenziato

Dipartimento Lavoro, Formazione Professionale e Politiche Sociali
Settore 5
Pari opportunità
Politiche di genere
~~Volontariato~~
Servizio civile
e Immigrazione

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Valutazione: Accettabile

I dati sono esatti e aggiornati?

I dati personali sono forniti dai dipendenti, all'atto dell'autocertificazione. Gli eventuali aggiornamenti sono forniti dagli stessi in sede di rinnovo della richiesta di verifica per scadenza di validità del Certificato del Casellario Giudiziale, tenendo conto delle modalità stabilite nel Piano Triennale di Prevenzione della Corruzione e Trasparenza – Aggiornamento Annuale.

I dati giudiziari sono forniti dall'Amministrazione della Giustizia, secondo le risultanze delle proprie banche dati.

Valutazione: Accettabile

Qual è il periodo di conservazione dei dati?

Il periodo di conservazione dei dati è legato ai possibili controlli da parte degli organi a ciò deputati per cui è di non meno di cinque anni

Valutazione: Accettabile

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Il Consenso espresso al trattamento ed alla comunicazione dei propri dati personali è allegato all'autocertificazione di cui al DPR 445/2000 prodotta dai dipendenti in relazione agli obblighi di prevenzione della corruzione stabiliti dal PTPCT 2019/2021 e relativi aggiornamenti annuali.

Valutazione: Migliorabile

Piano d'azione / misure correttive:

Prevedere momenti dedicati alla informazione ai dipendenti in materia di trattamento dei dati personali e giudiziari e relativi aggiornamenti

Ove applicabile? Come si ottiene il consenso degli interessati?

Settore Lavoro, Formazione Professionale e Politiche Sociali
Pari opportunità
Politiche di genere
Volontariato
Servizio civile
e Immigrazione

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Mediante rilascio di consenso per iscritto
Valutazione: Migliorabile **Piano d'azione / misure correttive:** Prevedere una modulistica standard e ad hoc per il rilascio del consenso al trattamento dei dati giudiziari.

Come fanno gli interessati ad esercitare i loro diritti di accesso e di portabilità dei dati? Inviando una mail alla Regione Calabria
Valutazione: Accettabile

Come fanno gli interessati ad esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)? Inviando una mail alla Regione Calabria
Valutazione: Accettabile

Come fanno gli interessati ad esercitare i loro diritti di limitazione e opposizione? Inviando una mail alla Regione Calabria
Valutazione: Accettabile

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto? La circolare nr. 265973/SIAR del 31/07/2018, prevede l'obbligo generalizzato, in capo al Titolare del Trattamento, e per esso ai Responsabili del Trattamento della segnalazione all'autorità di controllo nel caso di *Data Breach*. In particolare viene descritta la procedura da seguire al verificarsi una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Lavoro, Formazione Professionale e Politiche sociali
Settore 5
Pari opportunità
Politiche di genere
~~Volontariato~~
Servizio civile
e Immigrazione

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Valutazione: Accettabile

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di protezione equivalente Non è previsto il trasferimento dei dati al di fuori dell'UE
Valutazione: Accettabile

Come sono informati del trattamento gli interessati?
Valutazione: Accettabile

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Rischi

Misure esistenti o pianificate

Accesso riservato da password

I dati contenuti nei fascicoli sono conservati in armadi chiusi a chiave a cura del dipendente incaricato. Le richieste di verifica al Casellario e relative risultanze, sono inviati/ricevuti tramite Pec istituzionale del Settore regionale e acquisiti ufficialmente al protocollo generale. I dati di accesso alla Pec (Utenza e Password) sono personali. L'accesso ai Computer di tutti gli abilitati alla gestione della Pec sono protetti da password. Le password di accesso alla Pec ed ai computer devono essere attentamente custodite e modificate periodicamente.

Valutazione: Accettabile

Limitazione della permanenza dei file di dati sul server

I messaggi di trasmissione via Pec, sono detenuti sul server di WEBPEC Organizer della Regione Calabria per un tempo illimitato, non consentendo il sistema l'eliminazione dei messaggi inviati. Le richieste di verifica sono trasmesse, per conoscenza sulla mail personale, al responsabile del procedimento e al dirigente di settore.

Il personale incaricato alla gestione della posta elettronica certificata è informato del tassativo divieto alla lettura delle certificazioni allegate alle pec trasmesse dagli Uffici giudiziari, che come detto devono essere tempestivamente inoltrate alla casella di posta elettronica istituzionale del dirigente e del Responsabile AA.GG. di Settore. Quest'ultimo provvede direttamente alla protocollazione riservata e alla stampa in sicurezza e ad attuare tutte le altre misure idonee alla riservatezza del dato già descritte, ivi compresa la eliminazione del messaggio di invio dalla casella di posta elettronica personale sulla propria casella di p.e.. Alla cancellazione del messaggio sulla propria casella di posta elettronica istituzionale provvede il dirigente, una volta letto e valutato.

La stampa protocollata del certificato giudiziale è conservata in busta chiusa, firmata e timbrata sui lembi, tenuta in appositi fascicoli all'interno di armadi chiusi a chiave, a cura del personale autorizzato.

Valutazione: Migliorabile

Piano d'azione /misure correttive

Agli Uffici giudiziari (Casellario giudiziale competente) verrà richiesto di inviare preliminarmente un avviso sulla casella di posta elettronica certificata del Settore circa la disponibilità della certificazione richiesta che dovrà essere successivamente inviata esclusivamente all'indirizzo di posta elettronica

Settore 5
Pari opportunità
Politiche di genere
Volontariato
Servizio civile
e Immigrazione

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

istituzionale del Responsabile del Procedimento. In tal modo si avrà traccia del riscontro da parte degli Uffici giudiziari alla richiesta dell'ufficio escludendo, tuttavia, accessi accidentali ovvero non autorizzati delle certificazioni acquisite.

Accesso illegittimo ai dati

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

Una violazione di tali dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni, materiali o immateriali, ad esempio perdita del controllo dei dati personali o limitazione dei diritti, discriminazione, perdite finanziarie, pregiudizio alla reputazione. Attraverso accessi non autorizzati e abusivi dei dati della persona fisica, i membri della sua famiglia o conoscenti, o colleghi di lavoro, potrebbero venire a conoscenza, dell'eventuale presenza di iscrizioni sul Casellario Giudiziale che potrebbero dar luogo a comportamenti discriminatori da parte della società e nell'ambiente lavorativo, compresi atteggiamenti di diffidenza o pregiudizio, con conseguentemente compromissione dei rapporti di fiducia e di stima all'interno del gruppo e della serenità relazionale. Ciò probabilmente potrebbe avere risvolti anche gravi sulla salute psico-fisica dell'interessato e sui membri della sua stretta cerchia familiare.

Quali sono le principali minacce che potrebbero concretizzare i rischio?

Conoscenza dei dati da accesso abusivo al sistema informatico di Pec dell'Ente ;

Conoscenza dei dati da accesso abusivo ai computer in dotazione al Settore;

Quali sono le fonti di rischio?

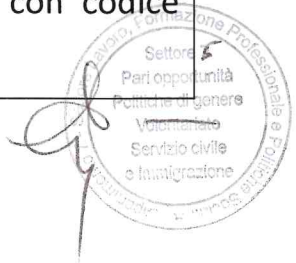
Soggetti esterni all'amministrazione che accedono abusivamente al sistema WEBPEC, soggetti esterni all'Amministrazione che apprendano copie delle pratiche cartacee in lavorazione. Soggetti interni all'Amministrazione che accedono ai computer in dotazione e ai supporti informatici di archiviazione.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Limitazione della permanenza sulle e-mail istituzionali personali;

Accessi ai Computer personali, riservati da password.

Impossibilità di ricerca diretta del protocollo in entrata, annotato con codice riservato. Accesso al protocollo tramite autenticazione.



Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

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

Importante. I dati personali e giudiziari dei dipendenti se posti a conoscenza di terzi possono comportare gravi conseguenze per l'onore, la reputazione e la dignità dei titolari di tali dati, anche a livello lavorativo, nonché conseguenze sullo stato di salute psico-fisica.

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

Trascurabile: I dati sono conservati in forma cartacea, protetti e custoditi in fascicoli e armadi chiusi a chiave. Le mail in entrata e uscita sono cancellate dalle e-mail personali comunque accessibili tramite utenze protette da password. Le pec presenti sul sistema WEBPEC sono consultabili solo con utenze personali. L'accesso ai computer personali è protetto da Password. Tutte le Password del settore sono modificate periodicamente.

Valutazione: Migliorabile

Piano d'azione / misure correttive:
- Modificare con media frequenza le credenziali di accesso su server WEBPEC da parte degli operatori, al fine di evitare il permanere della conoscenza di tali credenziali nell'ipotesi di cessazione delle relative mansioni;

Alla luce del Piano d'azione, come valutate *la gravità di questo rischio* (Accesso illegittimo ai dati)? Trascurabile;

Alla luce del Piano d'azione, come valutate *la probabilità di questo rischio* (Accesso illegittimo ai dati)? Trascurabile;

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Importante. Per i diretti interessati l'impatto comporterebbe grave nocumento e pregiudizio sia sul posto di lavoro sia nella propria vita relazionale. Per l'Amministrazione pubblica la fiducia da parte dei cittadini nell'inviolabilità dei sistemi a tutela dei dati personali sarebbe compromessa a vantaggio, viceversa, di una certa vulnerabilità con danno all'immagine

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

La modificazione accidentale o dolosa dei dati è improbabile. Le certificazioni contenenti i dati giudiziari, devono permanere per almeno un quinquennio all'interno dei fascicoli cui fanno riferimento per eventuali verifiche da parte degli organi deputati al controllo, ragion per cui risulta importante che sia garantita la loro conservazione e la loro integrità.

All'uopo i dati sono conservati in formato cartaceo e riportano il numero e la data di protocollo. Sono inseriti anche sul sistema di protocollazione dell'Ente, in formato PDF e in modalità riservata, quindi non accessibile. Le Pec in entrata e in uscita contengono allegati in formato PDF immodificabile.

Valutazione: Migliorabile

Piano d'azione / misure correttive

Al fine di garantirne la conservazione e l'integrità, si prevede di effettuare il back up dei dati su CD-Rom, Hard-Disk esterno o Chiavetta USB. I file copiati saranno conservati a cura del Responsabile del procedimento e del Dirigente in modo da consentire in ogni momento la verifica della loro integrità.

Quali sono le fonti di rischio?

Non se ne ravvedono

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

Accesso riservato con password, custodia in sicurezza, file pdf immodificabili, back up dei dati, copia su supporti informatici esterni.

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

Trascurabile. Le possibilità di modificazione del dato risulta altamente improbabile alla luce delle misure previste.

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

Trascurabile. Il rischio di modifica dei dati è altamente improbabile alla luce delle misure previste.

Valutazione: Accettabile

Settore Lavoro, Formazione Professionale e Politiche Sociali
Settore 5
Pari opportunità
Politiche di genere
Volontariato
Servizio civile
e immigrazione

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Alla luce del Piano d'azione, come valutate *la gravità di questo rischio* (Modifiche indesiderate dei dati)? Trascurabile; Alla luce del Piano d'azione, come valutate *la probabilità di questo rischio* (Modifiche indesiderate dei dati)? Trascurabile;

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?
Non se ne ravvedono. La P.A. potrebbe invece dover giustificare l'eventuale attribuzione di incarichi e nomine in assenza di riscontri sulle autocertificazioni in caso di controlli da parte dell'Autorità Anticorruzione.

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?
Problemi tecnici sul server WEBPEC organizer della Regione Calabria, accessi indesiderati sui server, rottura macchine e supporti informatici di archiviazione, riorganizzazioni della struttura regionale

Quali sono le fonti del rischio?
Hackeraggio e obsolescenza, senescenza e guasto hardware, smarrimento documenti dovuti a modifiche logistiche

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?
Back up di sicurezza, accesso ai file e alle pec riservato da password.

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?
Trascurabile per i dipendenti.
Importante per la PA che potrebbe non assolvere ai doveri di controllo

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

Valutazione: Migliorabile
Piano d'azione – misure correttive
- Prevedere il back up, la conservazione su CD- Rom o Chiavetta USB, dei dati in modo da duplicare la conservazione. I file copiati saranno conservati a cura del Responsabile del procedimento e del Dirigente.

- Aumentare la frequenza di back up.

Alla luce del Piano d'azione, come valutate la gravità di questo rischio (Perdita dei dati)? Trascurabile;

Alla luce del Piano d'azione, come valutate la probabilità di questo rischio (Perdita dei dati)? Trascurabile;

Settore 5
Pari opportunità
Politiche di genere
Volontariato
Servizio civile
e Immigrazione

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Piano d'azione

Panoramica

Contesto
Panoramica del trattamento
Principi Fondamentali
Finalità
Basi legali
Adeguatezza dei dati
Esattezza dei dati
Periodo di conservazione
Misure a tutela dei diritti degli interessati
Informativa
Raccolta del consenso
Diritto di rettifica e diritto di cancellazione
Diritto di limitazione e diritto di opposizione

Responsabili del trattamento

Misure esistenti
Accesso riservato da password
Limitazione alla permanenza dei dati su server

Rischi
Accesso illegittimo ai dati
Modifiche indesiderate dei dati
Perdita dei dati

Misure Migliorabili
Misure Accettabili

Contesto

Panoramica del trattamento

Piano d'azione / misure correttive:

Particolari cautele devono essere adottate in riferimento al trattamento del dato giudiziario che può presentare un rischio elevato per i diritti e le libertà della persona fisica. Tenendo conto che non sembra sufficiente informare il dipendente della misura di controllo e acquisirne il relativo consenso, si ritiene utile provvedere alla conservazione dei dati su appositi supporti esterni (CD-rom- Hard Disk) custoditi dal personale autorizzato. Il responsabile del procedimento adotta opportune misure atte al rispetto della norma a salvaguardia dell'accesso accidentale ovvero non autorizzato. In particolare il RUP si attiene a tutte le disposizioni regionali sulla sicurezza dei dati, anche secondo le disposizioni regionali vigenti. Nella richiesta di dati giudiziari il RUP circoscrive la richiesta ai soli dati necessari relativi ad eventuali reati previsti nel capo I, del titolo II, del libro secondo del codice penale.

Data prevista implementazione: 31/12/2019

Responsabile dell'implementazione: Responsabile del Procedimento

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Principi fondamentali

Misure a tutela dei diritti degli interessati

Piano d'azione – misure correttive

Prevedere momenti dedicati alla informazione ai dipendenti in materia di trattamento dei dati personali e giudiziari e relativi aggiornamenti

Data prevista implementazione: 31/12/2019

Responsabile dell'implementazione: Dirigente Settore Pari Opportunità

Rischi

Limitazione della permanenza dei file di dati sul server

Piano d'azione / misure correttive:

Agli Uffici giudiziari (Casellario giudiziale competente) verrà richiesto di inviare preliminarmente un avviso sulla casella di posta elettronica certificata del Settore circa la disponibilità della certificazione richiesta che dovrà essere successivamente inviata esclusivamente all'indirizzo di posta elettronica istituzionale del Responsabile del Procedimento. In tal modo si avrà traccia del riscontro da parte degli Uffici giudiziari alla richiesta dell'ufficio escludendo, tuttavia, accessi accidentali ovvero non autorizzati delle certificazioni acquisite.

Data prevista implementazione: 31/12/2019
Responsabile dell'implementazione:
Dirigente Settore Pari Opportunità/Responsabile del Procedimento

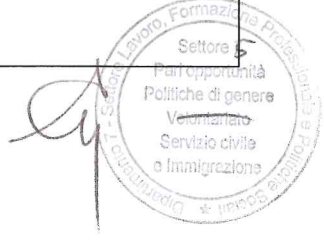
Alla luce del piano d'azione, come valutate la gravità di questo rischio (Accesso illegittimo ai dati)? **Trascurabile**
Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Accesso illegittimo ai dati)? **Trascurabile**

Accesso illegittimo ai dati

Piano d'azione / misure correttive:

Modificare con media frequenza le credenziali di accesso su server WEBPEC da parte degli operatori, al fine di evitare il permanere della conoscenza di tali credenziali nell'ipotesi di cessazione delle relative mansioni;

Data prevista implementazione: 31/12/2019



Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Responsabile dell'implementazione: Dipendenti/Responsabile del Procedimento

Alla luce del Piano d'azione, come valutate *la gravità di questo rischio* (Accesso illegittimo ai dati)? **Trascurabile**;

Alla luce del Piano d'azione, come valutate *la probabilità di questo rischio* (Accesso illegittimo ai dati)? **Trascurabile**;

Modifiche indesiderate dei dati
Piano d'azione / misure correttive:
Al fine di garantirne la conservazione e l'integrità, si prevede di effettuare il back up dei dati su CD-Rom, Hard-Disk esterno o Chiavetta USB. I file copiati saranno conservati a cura del Responsabile del procedimento e del Dirigente in modo da consentire in ogni momento la verifica della loro integrità.

Data prevista implementazione: 31/12/2019
Responsabile dell' implementazione:
Dirigente Settore Pari Opportunità/Responsabile del Procedimento

Alla luce del Piano d'azione, come valutate la gravità di questo rischio (Modifiche indesiderate dei dati)? **Trascurabile**;
Alla luce del Piano d'azione, come valutate la probabilità di questo rischio (Modifiche indesiderate dei dati)? **Trascurabile**;

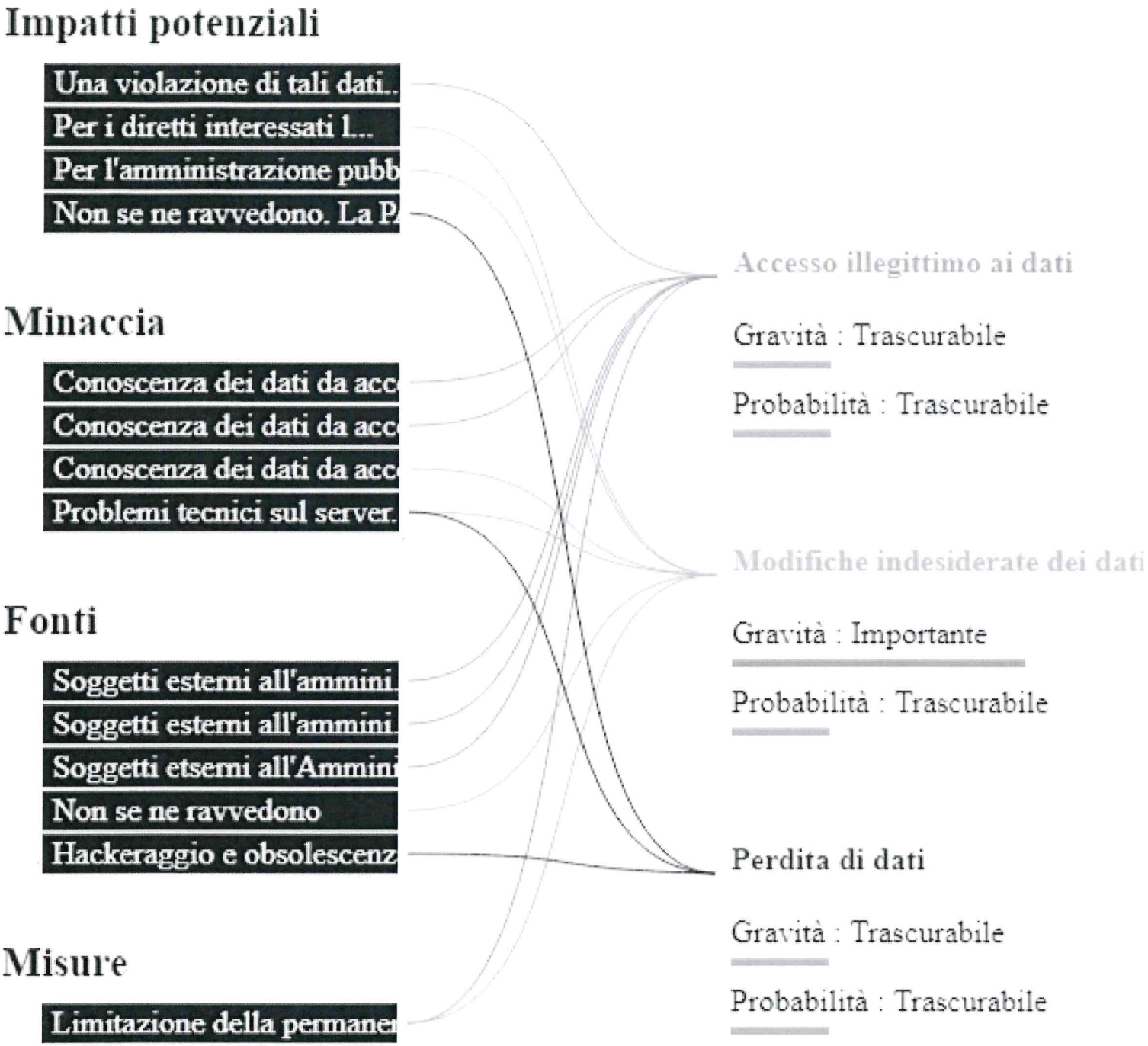
Perdita dei dati
Piano d'azione / misure correttive:
- Prevedere il back up, la conservazione su CD- Rom o Chiavetta USB, dei dati in modo da duplicare la conservazione. I file copiati saranno conservati a cura del Responsabile del procedimento e del Dirigente.
- Aumentare la frequenza di back up.

Data prevista implementazione: 31/12/2019
Responsabile dell' implementazione:
Dirigente Settore Pari Opportunità/Responsabile del Procedimento

Alla luce del Piano d'azione, come valutate la gravità di questo rischio (Perdita dei dati)? **Trascurabile**;
Alla luce del Piano d'azione, come valutate la probabilità di questo rischio (Perdita dei dati)? **Trascurabile**;

Settore 5
Pari opportunità
Politiche di genere
Volontariato
Servizio civile
e Immigrazione

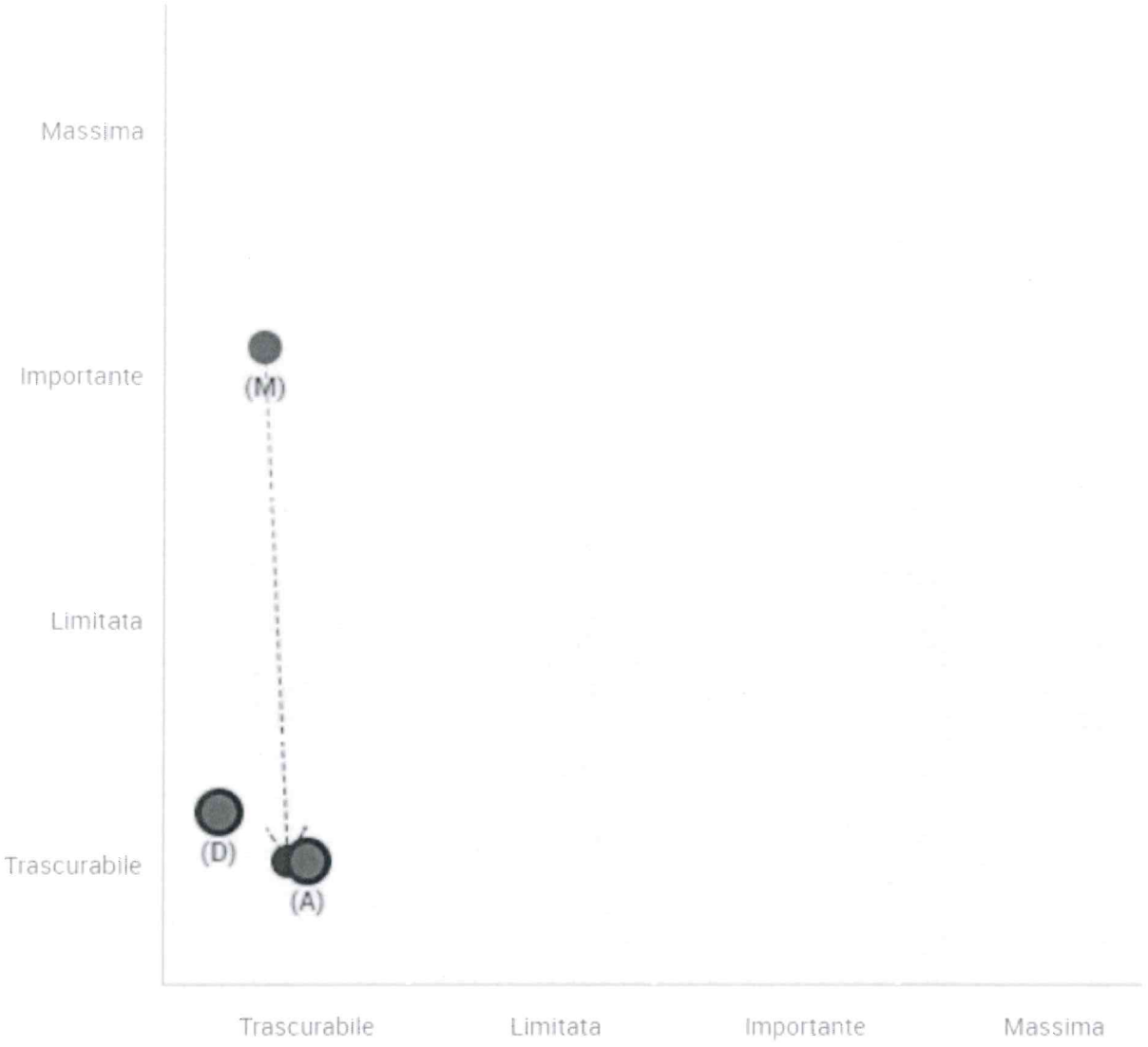
Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.



Settore 5
Pari opportunità
Politiche di genere
Volontariato
Servizio civile
Immigrazione

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Gravità del rischio



Probabilità del rischio

- Misure pianificate o esistenti
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

28/08/2019

Settore 5
Pari opportunità
Politiche di genere
~~Volontariato~~
Servizio civile
e Immigrazione

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Informazioni sulla PIA

Nome della PIA Protezione Dati destinatari Corsi di Alfabetizzazione Progetto Calabria Friends - Fondo Asilo Migrazione e Integrazione 2014-2020 e degli Ospiti per il progetto INCIPIT.

Nome autore	Vito Samà

Nome valutatore	Edith Macrì

Nome validatore	Roberto Cosentino

Data creazione	... /09/2019

Nome del DPO/RPD	Angela Stellato

Parere del DPO/RPD	POSITIVO (nota n. 335014 del 27/09/2019)

Richiesta del parere degli interessati E' stato chiesto il consenso degli interessati. E' stato autorizzato dagli stessi il trattamento dei dati personali forniti, ai sensi del D.Lgs. nr. 196/2003 e successivi.

Motivazione della mancata richiesta del parere degli interessati

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Contesto

Panoramica del trattamento

Qual è il trattamento in considerazione?

Gestione dati personali dei destinatari dei corsi di alfabetizzazione erogati dalle scuole individuate come partners della Regione Calabria nell'ambito del progetto Calabria Friends, nonchè dei dati degli ospiti per il progetto INCIPIT (Iniziativa Calabra per l'Identificazione, Protezione ed Inclusione sociale delle vittime di Tratta).

I dati acquisiti dalle scuole partners vengono inviati dalle stesse alla Regione Calabria, in particolare alla mail istituzionale del Responsabile del Procedimento, per il successivo invio all'Autorità delegata del Fami – Ministero dell'Interno, mediante procedura on line di caricamento dei dati. L'acquisizione di tali dati ha tra l'altro la finalità di disporre di un quadro periodicamente aggiornato sui destinatari e sui macroservizi da essi fruiti nell'ambito degli interventi finanziati dal Fondo Asilo Migrazione ed Integrazione 2014-2020. Tale attività è necessaria e funzionale alla restituzione dell'andamento del Fondo alla Commissione Europea così come previsto nei regolamenti UE 516 e 514/2014 FAMI. Per quanto riguarda il progetto INCIPIT, vengono comunicati alla Regione i registri delle presenze degli ospiti presso le strutture degli Enti partners selezionati della Regione Calabria, ai fini della sola rendicontazione.

Quali sono le responsabilità connesse al trattamento?

Il Responsabile del Procedimento, assume cognizione dei dati personali dei beneficiari, trasmessi in tabelle dalle scuole eroganti i corsi di alfabetizzazione, nonché il registro delle presenze degli ospiti presso le strutture, per i quali comunque vengono trasmessi solo le iniziali del nome e cognome.Tali dati devono essere accuratamente trattati e conservati onde evitare indebiti accessi dall'esterno e da parte di soggetti non deputati a farlo.

Ci sono standard applicabili al trattamento?

Il Responsabile del procedimento è tenuto a garantire, la riservatezza dei dati, attraverso un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).Cura la conservazione dei file trasmessi sul suo indirizzo di posta istituzionale. In particolare, vengono adottate particolari cautele nella gestione dei sistemi informatici. Difatti, i dati ricevuti, non vengono protocollati in entrata, in modo da non essere rintracciabili con semplice ricerca diretta, preso atto del fatto che il sistema di protocollazione dell'Ente prevede anche il caricamento del relativo file. I file, inoltre, sono custoditi dal Responsabile del Procedimento e non inoltrati per conoscenza su altre mail – PEC, ad eccezione del Dirigente di Settore che ne prende visione su richiesta.

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Principi fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Con Decreto prot. n. 19738 del 24/12/2015, l'Autorità Responsabile ha adottato l'Avviso pubblico per la presentazione di progetti finanziati a valere sul Fondo Asilo, Migrazione e Integrazione 2014-2020, di cui la Regione Calabria è risultata beneficiaria.

Considerato che la Regione Calabria ha presentato il progetto INCIPIT a tutela delle vittime di Tratta di cui al Programma unico di emersione, assistenza ed integrazione sociale a favore degli stranieri e dei cittadini di cui al comma 6 bis dell'art. 18 del decreto legislativo 25 luglio 1998, nr. 286, alle vittime dei reati previsti dagli art. 600 e 601 del codice penale, o che versano nelle ipotesi di cui al comma 1 del medesimo art. 18 ed è stata selezionata per più annualità in merito allo stesso.

Il trattamento dei dati risulta necessario al fine di consentire all'Ente regionale, di adempiere al monitoraggio trimestrale mediante inserimento dei dati dei destinatari dei corsi di alfabetizzazione sulla piattaforma ministeriale, ai fini dei successivi adempimenti da parte dell'Autorità del FAMI. Ai fini della rendicontazione viene altresì comunicato il numero dei destinatari. Per quanto concerne il progetto INCIPIT i dati vengono acquisiti ai fini della rendicontazione.

Valutazione: Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Il trattamento dei dati personali è considerato lecito sulla base dell'articolo 6, lett. a) ed f) , del GPDR 679/2016 e deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri prevedere garanzie appropriate per i diritti e le libertà degli interessati. In particolare cautele sono applicate se l'interessato è un minore. Difatti in tal caso, per garantirne l'anonimato, nelle tabelle relative ai destinatari vengono riportate solo le iniziali del Nome e del Cognome.

Nel caso di soggetti vittime di tratta, l'anonimato è garantito mediante l'indicazione nei registri degli ospiti delle sole iniziali del nome e del cognome.

La base normativa legittimante il trattamento dei dati per le finalità del Progetto Calabria Friends , si rinviene nei seguenti atti e riferimenti legislativi:

- GPDR nr. 679/2016;
- Regolamento (UE) N. 514/2014 del Parlamento Europeo e del Consiglio del 16 aprile 2014 recante disposizioni generali sul Fondo Asilo, Migrazione e Integrazione (FAMI) 2014-2020 e sullo strumento di sostegno finanziario per

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

I dati personali sono forniti dai destinatari dei corsi di alfabetizzazione, o dagli ospiti delle strutture all'atto della compilazione della scheda anagrafica. Gli eventuali aggiornamenti sono a cura delle scuole e delle strutture ospitanti e sono trasmessi al RUP.
Valutazione: Accettabile

Qual è il periodo di conservazione dei dati?
Il periodo di conservazione dei dati è legato ai possibili controlli da parte degli organi a ciò deputati per cui è di non meno di cinque anni.
Valutazione: Accettabile

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?
Il Consenso espresso al trattamento dei dati ai sensi del D.lgs. 196/2003 e ss.mm.ii., viene riportato in calce alla scheda compilata a cura del destinatario.
Valutazione: Accettabile

Ove applicabile? Come si ottiene il consenso degli interessati?
Mediante rilascio di consenso per iscritto
Valutazione: Accettabile

Come fanno gli interessati ad esercitare i loro diritti di accesso e di portabilità dei dati?
Inviando una comunicazione alla Regione Calabria
Valutazione: Accettabile

Come fanno gli interessati ad esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Dipartimento Lavoro, Formazione, Politiche sociali
Settore 5
Pari opportunità
Politiche di genere
Servizio civile
e immigrazione

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Rischi

Misure esistenti o pianificate

Accesso riservato da password

I dati contenuti nei file pervenuti sotto forma di tabelle e registri, sono trasmessi alla mail istituzionale del RUP, sono scaricati e conservati sul PC dello stesso. L'accesso al Computer del RUP è protetto da password. I file permangono sulla mail istituzionale dello stesso e inoltrati al Dirigente di settore su richiesta. I dati di accesso alla mail istituzionale (Utenza e Password) sono personali. Le password di accesso alla mail ed al computer deve essere attentamente custodite e modificate periodicamente.

Valutazione: Accettabile

Limitazione della permanenza dei file di dati sul server

I file ricevuti dal Rup, permangono sulla sua mail istituzionale per un tempo illimitato. Gli stessi sono inoltrati sulla mail istituzionale del Dirigente, se richiesti, e cancellati periodicamente.

Valutazione: Migliorabile

Piano d'azione /misure correttive

Al fine di limitare la permanenza dei file sulla mail del RUP e della dirigente, si pianifica la stampa cartacea degli stessi e la loro conservazione in fascicoli e in armadi chiusi a chiave. Alla cancellazione dei file di cui trattasi provvedono il RUP ed eventualmente il dirigente una volta letti e valutati. I file vengono inviati altresì all'operatore deputato al caricamento dei dati sulla piattaforma ministeriale per quanto concerne il progetto Fami; Anche in questo caso i file vengono cancellati dopo l'adempimento.

Accesso illegittimo ai dati

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

In caso di illegittimi accesso ai dati, i rischi per i diritti e le libertà delle persone fisiche potrebbero avere probabilità e gravità diverse. Potrebbero derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare il trattamento può comportare discriminazioni, furto o

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

limitati i loro diritti e le loro libertà, considerato che spesso si tratta di persone in fuga dai paesi di origine. Nonché conseguenze sul loro stato di salute psico-fisica, trattandosi spesso di persone già oggetto di violenze e ingiustizie soprattuto per quanto concerne le vittime di tratta.

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

Trascurabile: I file pervenuti sull'e-mail istituzionali del Rup sono unicamente inoltrate al Dirigente su richiesta; le caselle di e-mail personali sono comunque accedibili tramite utenze protette da password. L'accesso ai computers personali è protetto da Password. Le password sono modificate periodicamente.

Valutazione: Migliorabile

Piano d'azione / misure correttive:
- Modificare con media frequenza le credenziali di accesso alle e-mail istituzionali, al fine di evitare il permanere della conoscenza di tali credenziali nell'ipotesi di cessazione delle relative mansioni;
Alla luce del Piano d'azione, come valutate *la gravità di questo rischio* (Accesso illegittimo ai dati)? Trascurabile;

Alla luce del Piano d'azione, come valutate *la probabilità di questo rischio* (Accesso illegittimo ai dati)? Trascurabile;

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Trascurabile. Per i diretti interessati l'impatto potrebbe essere di scarsa importanza. Per l'Amministrazione Pubblica la fiducia da parte dei cittadini nell'inviolabilità dei sistemi a tutela dei dati personali sarebbe compromessa a vantaggio, viceversa, di una certa vulnerabilità con danno all'immagine.

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

La modificazione accidentale o dolosa dei dati è improbabile.

All'uopo i dati sono conservati in formato digitale sull' Hard- Disk del RUP. Sono inseriti anche sulla piattaforma ministeriale al fine degli adempimenti previsti. L'accesso alla procedura richiede l'autenticazione con utenza e password

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

(Modifiche indesiderate dei dati)? Trascurabile;

Settore 5
Pari opportunità
Politiche di genere
Volontariato
Servizio civile
e Immigrazione

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?
Non se ne ravvedono. La P.A. potrebbe invece dover giustificare l'eventuale perdita dei dati a seguito di controlli da parte degli organi deputati tra cui anche l'autoritò delegata del FAMI 2014-2020 e da parte della Presidenza del Consiglio dei Ministri – Dipartimento per le Pari Opportunità.

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?
Problemi tecnici sul server di posta elettronica istituzionale, accessi indesiderati sul server, rottura macchine e supporti informatici di archiviazione, riorganizzazioni della struttura regionale;

Quali sono le fonti del rischio?
Hackeraggio e obsolescenza, senescenza e guasto hardware;

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?
Back up di sicurezza, accesso ai file e alle caselle di posta elettronica istituzionale, riservato da password.

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?
Trascurabile per i destinatari.
Importante per la PA che potrebbe non assolvere ai doveri di controllo

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

Valutazione: Migliorabile
Piano d'azione – misure correttive
- Prevedere il back up, la conservazione su CD- Rom o Chiavetta USB, dei dati in modo da duplicare la conservazione. I file copiati saranno conservati a cura del Responsabile del procedimento e del Dirigente.

-Prevedere la conservazione dei dati in formato cartaceo in armadi chiusi a chiave.

- Aumentare la frequenza di back up.

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Piano d'azione

Panoramica

Principi fondamentali
Panoramica del trattamento
Finalità
Basi legali
Adeguatezza dei dati
Esattezza dei dati
Periodo di conservazione
Misure a tutela dei diritti degli interessati
Informativa
Raccolta del consenso
Diritto di rettifica e diritto di cancellazione
Diritto di limitazione e diritto di opposizione
Responsabili del trattamento

Limitazione alla permanenza dei dati su server esterni

Rischi
Accesso illegittimo ai dati
Modifiche indesiderate dei dati
Perdita di dati

Misure esistenti

Misure Migliorabili
Misure Accettabili

Principi fondamentali

Panoramica del trattamento

Piano d'azione / misure correttive:

Particolari cautele devono essere adottate in riferimento al trattamento del dati in questione, poiché trattasi di dati forniti da persone immigrate per i quali esiste nel caso delle vittime di tratta un programma unico di emersione, assistenza ed integrazione sociale a favore degli stranieri e dei cittadini di cui al comma 6 bis dell'art. 18 del decreto legislativo 25 luglio 1998, nr. 286, alle vittime dei reati previsti dagli art. 600 e 601 del codice penale, o che versano nelle ipotesi di cui al comma 1 del medesimo art. 18. Si auspica la conservazione dei dati, su appositi supporti esterni (CD-rom - Hard Disk- Chiavetta USB) custoditi dal personale autorizzato, oltre che la stampa cartacea degli stessi, al fine di procedere alla cancellazione periodica delle e-mail pervenute al RUP.

Data prevista implementazione: 31/12/2019

Responsabile dell'implementazione: RUP

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Piano d'azione / misure correttive:

Al fine di garantirne la conservazione e l'integrità, si prevede di effettuare il back up dei dati su CD-Rom, Hard-Disk esterno o Chiavetta USB. I file copiati saranno conservati a cura del Responsabile del procedimento e del Dirigente in modo da consentire in ogni momento la verifica della loro integrità.

Si prevede anche la stampa degli stessi in formato cartaceo e la loro custodia in armadi chiusi a chiave, in modo da poter verificare in ogni momento la loro integrità.

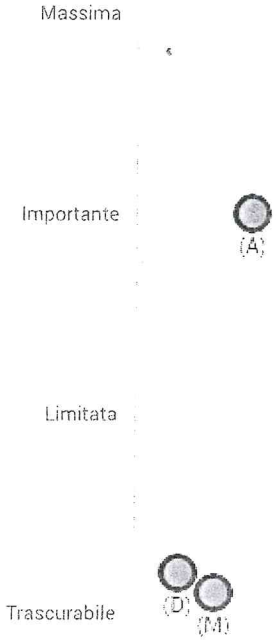
I file ricevuti devono essere convertiti prima di essere copiati in formato PDF immodificabile, in modo da garantirne l'integrità e la immodificabilità accidentale e dolosa.

Data prevista implementazione: 31/12/2019
Responsabile dell'implementazione: Dirigente Settore/RUP

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Mappaggio dei rischi

Gravità del rischio



Trascurabile | Limitata | Importante | Massima

Probabilità del rischio

- Misure pianificate o esistenti
- **Con le misure correttive implementate**
- **(A)ccesso illegittimo ai dati**
- **(M)odifiche indesiderate dei dati**
- **(P)erdita di dati**

28/08/2019

Dipartimento 1 - Settore Lavoro, Formazione Professionale e Politiche Sociali
Settore Pari opportunità Politiche di genere Volontariato Servizio civile e immigrazione

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.

Impatti potenziali

In caso di illeggittimi acc...
Per i diretti interessati l...
Per l'amministrazione pubb
Non se ne ravvedono. La P

Minaccia

Conoscenza dei dati da acc
Conoscenza dei dati da acc
Conoscenza dei dati da acc
Problemi tecnici sul server.

Fonti

Soggetti esterni all'ammini.
Non se ne ravvedono
Hackeraggio e obsolescenz

Misure

Accesso riservato da passw
Limitazione della permanen

Accesso illegittimo ai dati

Gravità : Importante

Probabilità : Trascurabile

Modifiche indesiderate dei dati

Gravità : Importante

Probabilità : Trascurabile

Perdita di dati

Gravità : Trascurabile

Probabilità : Trascurabile

Dipartimento 7 - Settore Lavoro, Formazione Professionale e Politiche Sociali
Settore 5
Pari opportunità
Politiche di genere
Volontariato
Servizio civile
e immigrazione

Copia informatica conforme ai sensi dell'art. 23-bis del CAD e s.m.