REGOLAMENTO CONSORTILE:

ART. 4 STATUTO LAVORATORI

ED UTILIZZO DI

STRUMENTI INFORMATICI

INDICE

1. Premessa..... pag. 02

2. Entrata in vigore del Regolamento e pubblicità pag.02

3. Obiettivi ..... pag. 02

4. Ambito di applicazione ..... pag. 03

5. Riferimenti Leggi e Regolamenti..... pag. 03

6. Definizioni ..... pag. 03

7. ART. 4 Statuto dei lavoratori ..... pag. 04

7.1 Strumenti necessari a rendere l'attività lavorativa Ex. Art. 4 comma 2 Statuto dei lavoratori .. pag. 05

8. Modalità operative degli strumenti elettronici..... pag. 06

8.1 Soggetti che possono utilizzare gli strumenti elettronici ..... pag. 06

8.2 Riservatezza delle informazioni..... pag. 07

8.3 Regole di utilizzo ..... pag. 07

8.4 Utilizzo postazioni di lavoro ..... pag. 08

8.5 Utilizzo pc portatili e dispositivi portatili (tablet, smartphone,etc) ..... pag. 11

8.6 Periferiche di archiviazione di massa ..... pag. 12

9. Protezione firewall, antivirus, antimalware, antiransomware..... pag. 13

10. Utilizzo di Internet..... pag. 14

11. Utilizzo posta elettronica..... pag. 14

12. Cessazione del rapporto di lavoro ..... pag. 16

13.Telefoni fissi, fax, stampanti e fotocopiatrici ..... pag. 17

14. Accesso ai dati trattati..... pag. 17

15. Possibilità di controlli e loro gradualità..... pag. 18

16. Casi di inottemperanza..... pag. 20

1. Premessa

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete internet dai personal computer, espone Co.va.r 14 e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto di autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'ente stessa.

Premesso, quindi, che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, Co.va.r 14 ha adottato il seguente Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Detto Regolamento sarà oggetto di successive revisioni ed estensioni ad altre tematiche relative alla privacy ed alla sicurezza dei dati, che sono attualmente oggetto di specifico esame.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite in sede di lettera di designazione a persona autorizzata al trattamento dei dati personali.

Considerato inoltre che Co.va.r 14, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha da tempo deciso di mettere a disposizione dei propri collaboratori che ne necessitassero per il tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti (computer portatili, telefonici cellulari, palmari, ecc.) sono state inserite nel Regolamento alcune clausole relative alle modalità ed ai doveri che ciascun collaboratore deve osservare nell'utilizzo di tale strumentazione.

2. ENTRATA IN VIGORE DEL REGOLAMENTO E PUBBLICITÀ

Il nuovo Regolamento è in vigore dal 20 aprile 2018.

Copia del Regolamento, oltre ad essere affisso nella bacheca consortile, verrà inviato a ciascun dipendente sulla mail consortile.

3. OBIETTIVI

Il presente Regolamento ha l'obiettivo di:

- definire i criteri per l'assegnazione a personale dipendente e non, di risorse ICT ad uso individuale e i relativi flussi autorizzativi;
- disciplinare le modalità di corretto utilizzo e conservazione delle risorse ICT sopra indicate;

- definire le modalità per la conservazione e l'utilizzo dei dati relativi all'uso delle risorse e servizi informatici consortili;
- stabilire ruoli e responsabilità dei soggetti coinvolti.

4. AMBITO DI APPLICAZIONE

Il presente Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e di livello, nonché a tutti i collaboratori dell'ente a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratori a progetto, in stage, ecc.).

5. RIFERIMENTI A LEGGI E REGOLAMENTI

- D.Lgs 196/03;
- Deliberazione 1° marzo 2007, n. 13- Lavoro: le linee guida del Garante per la posta elettronica e Internet" (Gazzetta Ufficiale n. 58 del 10 marzo 2007) e s.m.i.;
- Regolamento Europeo 2016/679;
- Raccomandazione 5/15 del Comitato dei Ministri avente ad oggetto il trattamento dei dati personali in ambito occupazionale;
- Garante Privacy " Linee guida per posta elettronica e internet" del 01.03.2007;
- Direttiva n. 2/2009 del Dipartimento della Funzione Pubblica ad oggetto: " Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro"
- Parere del Garante dell'11 ottobre 2018, Reg dei provvedimenti n. 464 dell' 11/10/2018: "parere sullo schema di disegno di legge "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo".

6. DEFINIZIONI

Ai fini del presente Regolamento si intende per :

Utente	ogni dipendente e collaboratore (lavoratore somministrato, in stage, ecc.) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "persona autorizzata al trattamento ".
Mezzi di telecomunicazione	sistemi mobili con tecnologia che consentono lo svolgimento di funzioni di telefonia e/o trasmissione dati e/o funzioni video

Risorse ICT ad uso individuale (o risorse ICT)	le risorse e servizi informatici e i mezzi di telecomunicazione forniti dall'ente per uso individuale
Tablet	sistema mobile con tecnologia che garantisce la trasmissione dati e funzioni video
Risorse e servizi informatici	qualsiasi tipo di hardware, mezzi di comunicazione elettronica, rete di trasmissione dati, software, informazioni in formato elettronico e, in generale, applicativi
Fax	servizio telefonico consistente nella trasmissione (invio e ricezione) di immagini fisse (tipicamente copie di documenti).

7. ART. 4 STATUTO LAVORATORI

Premessa

Il Co.va.r 14:

- Ha il diritto/ dovere di precisare ai sensi dell'art 4 comma 2 dello statuto dei lavoratori gli strumenti che l'ente ritiene necessari per svolgere la prestazione lavorativa;
- ha il diritto/dovere di indicare in modo chiaro e dettagliato le indicazioni sul corretto utilizzo degli strumenti messi a disposizione e se, in quale misura e con quali modalità possano essere effettuati eventuali controlli;
- non effettua controlli a distanza dell'attività dei dipendenti, ai sensi art. 4 dello Statuto dei lavoratori (L. n. 300/1970), mediante sistemi hardware e software finalizzati, ad esempio:
    - alla lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
    - all'analisi occulta di computer portatili eventualmente affidati in uso;
- privilegia, rispetto alle misure repressive, quelle organizzative e tecnologiche volte a prevenire utilizzi impropri degli strumenti, minimizzando in ogni evenienza l'uso dei dati riferibili ai dipendenti e comunque nel rispetto dei principi di necessità, pertinenza e non eccedenza, tenendo conto altresì della disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali;

- si impegna a rispettare la protezione dei dati personali attraverso il pieno rispetto del Regolamento Europeo 2016/679 nonchè delle linee Guida del Garante Italiano e del Gruppo dei Garanti europei 29.

7.1 SUGLI STRUMENTI NECESSARI A RENDERE L'ATTIVITÀ LAVORATIVA EX ART 4 COMMA 2 STATUTO LAVORATORI

A seguito dell'entrata in vigore dell'art. 23, D. Lgs. 14 settembre 2015 n. 151, che ha modificato l'art. 4, L. 20 maggio 1970 n. 300, è stata riformata la disciplina relativa agli impianti audiovisivi e agli altri strumenti da cui derivi anche la possibilità di controllo a distanza dei lavoratori.

Ai sensi del comma 2 del novellato art. 4 gli strumenti utilizzati dai lavoratori, per rendere la prestazione lavorativa nonché quelli finalizzati ad attestare gli accessi e presenze, **dai quali può derivare anche la possibilità di un controllo a distanza** non richiedono, per la loro applicazione, la sussistenza di esigenze organizzative, produttive, di sicurezza o di tutela del patrimonio consortile e non necessitano del preventivo accordo sindacale né dell'autorizzazione degli Uffici ministeriali (DTL o MINISTERO).

Gli strumenti che Co.va.r 14 considera necessari a svolgere la prestazione lavorativa, sono:

a) Smartphone;
b) Il personal computer (fisso e/o portatile) con i relativi software operativi e/o applicazioni istallate;
c) La rete informatica consortile;
d) La posta elettronica consortile con dominio @covar14;
e) I dispositivi di archiviazione hardware (c.d."storage");
f) Le periferiche consortili annesse (stampanti, fax, masterizzatori, supporti, magnetici, schede di connessione W-LAN, UMTS, ecc.);
g) Gli apparati di comunicazione fissi (telefoni, ecc.);
h) Tablet.

L'utilizzo degli strumenti sopra indicati può comportare l'acquisizione, da parte dell'Ente, dei dati relativi alla quantità della prestazione lavorativa svolta, nonché alle modalità e procedure di esecuzione della stessa.

Tali strumenti di lavoro sono affidati esclusivamente per l'esercizio delle funzioni assegnate, pertanto, non debbono essere utilizzati per uso personale o comunque estraneo all'attività

consortile, né modificati, ferma restando la possibilità di esplicita e preventiva autorizzazione da parte dell'Amministrazione.

Per maggiori dettagli sulle modalità di utilizzo degli strumenti sopra elencati si vedano i paragrafi successivi.

8. MODALITA' OPERATIVE DEGLI STRUMENTI ELETTRONICI

8.1 SOGGETTI CHE POSSONO UTILIZZARE GLI STRUMENTI ELETTRONICI

L'utilizzo delle risorse informatiche in generale, della posta elettronica e di Internet in particolare, come già anticipato, sono accordati al dipendente, all'apprendista, al collaboratore, allo stagista. L'utilizzo delle risorse (sistemi hardware, programmi e applicazioni software, apparati di rete, risorse di stampa, telefoni fissi, cellulari e tablet) è concesso solo in quanto strumenti di esecuzione delle normali prestazioni di lavoro o strumenti atti all'apprendimento del lavoro.

A tal fine, il lavoratore deve sempre mantenere comportamenti improntati alla massima diligenza, ed evitare abusi dei servizi e/o utilizzi contrari alle norme di legge, dei regolamenti consortili e alle regole definite dal presente Regolamento.

Non devono essere in nessun caso modificate o aggirate le configurazioni per la sicurezza o per il funzionamento, predisposte dalle funzioni tecniche sui dispositivi.

L'accesso alle, e l'utilizzo delle, risorse ICT dovrà essere limitato allo stretto indispensabile e comunque senza pregiudicare l'attività lavorativa e/o l'esecuzione contrattuale.

Non è consentito visualizzare, utilizzare e/o salvare file come musica, fotografie, film, materiale offensivo, illecito, inappropriato o in ogni caso contrario alla morale su server, aree condivise, strumenti di collaborazione di programmi informatici o su risorse informatiche consortili.

Le persone autorizzate alla manutenzione dei sistemi informatici hanno l'obbligo di svolgere solo le operazioni strettamente necessarie per adempiere al loro incarico, con divieto di svolgere attività di controllo a distanza, anche di propria iniziativa.

8.2 RISERVATEZZA DELLE INFORMAZIONI

La responsabilità di proteggere il patrimonio informativo consortile in coerenza con le norme di legge in vigore e con le procedure consortili coinvolge tutto il personale relativamente alle attività di competenza.

Tutti i supporti (chiavi USB, CD/DVD, elaboratori, ecc.) in uso al personale devono essere richiesti al personale IT.

Non è ammesso l'utilizzo di supporti personali.

Le periferiche di massa contenenti informazioni riservate devono essere protette in modo adeguato, conservandole ad esempio, quando non utilizzate, in vani chiusi a chiave, preservando la sicurezza della chiave stessa. In assenza di specifiche autorizzazioni, non devono, inoltre, venire duplicate e consegnate a terzi.

Il patrimonio informativo consortile registrato su dischi, nastri, ecc. non deve essere rimosso dal suo normale ambiente di conservazione in assenza di specifiche autorizzazioni della competente unità della funzione ICT. Gli elaborati e i supporti magnetici utilizzati all'esterno degli ambienti di lavoro devono essere conservati sotto la responsabilità dell'interessato e comunque riportati in sede per la loro archiviazione o distruzione.

Il reimpiego dei supporti di memorizzazione (hard disk, ecc.) può avvenire a condizione che il contenuto precedente non sia recuperabile (ad esempio cancellato tramite ripetute formattazioni o con funzionalità di prodotti specifici). In caso contrario, il supporto di memorizzazione deve essere distrutto.

8.3 REGOLE DI UTILIZZO

Al fine di garantire la funzionalità, la sicurezza ed il corretto impiego degli strumenti elettronici ed, al contempo, al fine di assicurare la protezione dei dati personali dei dipendenti, prevenire possibili contenziosi nonché contemperare le esigenze di un corretto svolgimento dell' attività lavorativa con quelle di tutela della sfera personale dei dipendenti si ritengono necessari i seguenti accorgimenti su:

A) GESTIONE DELLA PASSWORD

1. PROCEDURE CORRETTE

- modificare al primo accesso la password così che da quel momento, sia conosciuta solo dall'utente stesso;

- mantenere la password segreta nei confronti di chiunque compresi i colleghi di lavoro;
- sostituire la password anche in caso di semplice sospetto circa la venuta meno della sua segretezza;
- comporre le password con almeno 8 caratteri di cui almeno 4 delle seguenti tipologie :
    a) un carattere maiuscolo (da A a Z)
    b) un carattere minuscolo (da a a z)
    c) una cifra numerica (da 0 a 9)
    d) un carattere non alfanumerico, come ad esempio: !,$,#.
- modificare la password ogni 90 giorni.

L'utilizzo combinato del nome utente e della password attribuisce in modo univoco al singolo dipendente la responsabilità delle operazioni compiute.

2 PROCEDURE VIETATE:

- utilizzare password già in uso precedentemente;
- inserire all'interno della password anche solo parzialmente il nome dell'utente;
- impiegare le password utilizzate in ambito lavorativo in altre attività o situazioni richiedenti l'utilizzo di una password;
- ogni condotta che possa comprometterne la segretezza.

8.4 UTILIZZO POSTAZIONI DI LAVORO

1 . PROCEDURE CORRETTE

- utilizzare gli Strumenti ICT per il perseguimento di fini strettamente connessi agli incarichi lavorativi, e comunque coerentemente al tipo di attività svolta ed in linea con le disposizioni normative vigenti.;
- spegnere l'elaboratore ed eventuali periferiche (stampanti, scanner …) prima di lasciare l'ufficio al termine dell'attività lavorativa e, in generale, rispettare le istruzioni impartite dai produttori.

- attivare manualmente, prima di assentarsi dal proprio posto di lavoro, il blocco del personal computer seguendo queste istruzioni: cliccare contemporaneamente i tasti CTRL-ALT-CANC (DEL per i portatili), quindi cliccare sul pulsante "blocca computer";
- far eseguire le operazioni di manutenzione/riparazione degli Strumenti ICT solo da parte del personale autorizzato dalla Direzione ICT;
- archiviare la documentazione di lavoro, se possibile, all'interno di cartelle di rete ad accesso controllato sottoposte a programma di backup;

2. PROCEDURE VIETATE

- accedere al sistema informatico e mantenersi all'interno di esso per motivi non lavorativi o non di servizio;
- usare le risorse o i servizi in violazione di normative comunitarie, leggi, regolamenti, provvedimenti, prescrizioni, o per commettere attività illecite o discriminanti;
- modificare le configurazioni impostate;
- installare ed utilizzare prodotti software che non siano stati autorizzati dalla Direzione;
- installare, utilizzare software che consentano l'intercettazione automatica del traffico o la violazione delle password;
- usare le risorse o i servizi per scopi commerciali, promozionali, pubblicitari, senza aver ottenuto l'autorizzazione dalla propria direzione consortile;
- utilizzare eccessivo spazio disco o assorbire capacità di banda nei sistemi di telecomunicazione, attraverso la generazione o l'invio di mail non strettamente correlate all'attività lavorativa, o in generale, attraverso il trasferimento di file o messaggi di dimensioni eccessive;
- inviare o depositare sui server o sul disco del proprio computer materiale di natura illegale o discriminante;
- mascherare la propria identità all'interno dei sistemi informatici;
- utilizzare le credenziali di autenticazione di altri utenti, per qualsivoglia ragione;
- tentare di violare password o altri sistemi di protezione o tentare di superare le restrizioni imposte dal sistema;

- riprodurre o distribuire materiale consortile senza autorizzazione;
- copiare o modificare files, redatti da altri utenti, senza autorizzazione;
- alterare i dati, tentare di introdurre o diffondere virus, trojan, backdoor, dataminer o altri codici malefici;
- interferire con il corretto funzionamento o danneggiare le attrezzature di rete;
- intercettare o alterare qualunque tipo di dato o di comunicazione digitale.
- navigare su siti non correlati con la prestazione lavorativa (white list);
- effettuare download di programmi e files estranei al lavoro, salvo espressa autorizzazione scritta della Direzione (file musicali, video, audio) ;
- partecipare a forum (es.: facebook, etc), accedere e utilizzare chat line, partecipare ad aste on-line non correlate con l'attività operativa (es.: e-bay) in assenza di espressa autorizzazione scritta della Direzione;
- scaricare, copiare, conservare, diffondere file a contenuto offensivo, discriminatorio, pedofilo, o di altro contenuto illecito penalmente o civilmente;
- accedere a siti di gioco, pornografici o con finalità ludiche;
- attivare strumenti di chat in videochiamata (es.: skype/msn messenger) in assenza di espressa autorizzazione scritta della Direzione.

In caso di cambiamenti di unità organizzative o, in ogni caso, di trasferimenti dei dipendenti, le eventuali risorse ICT ad essi precedentemente assegnate sono sottoposte nuovamente a processo autorizzativo.

8.5 UTILIZZO PC PORTATILI E DISPOSITIVI PORTATILI (SMARTPHONE, TABLET)

1. PROCEDURE CORRETTE

- conservare in un luogo sicuro a fine giornata lavorativa;
- in caso di viaggi in aereo il portatile deve essere sempre trasportato come bagaglio a mano;

- quando il portatile viene lasciato in albergo deve essere consegnato al deposito valori o, quantomeno, riposto in una valigia o in un armadio chiusi a chiave;
- avvertire tempestivamente, in caso di furto di un elaboratore portatile, l'Ufficio IT, che darà le opportune indicazioni;
- prestare particolare attenzione all'utilizzo di elaboratori portatili in luoghi pubblici, quali ad esempio locali, stazioni e mezzi di trasporto;
- verificare, in caso di prolungato distacco dalla rete consortile, la disponibilità di aggiornamenti per il software antivirus e antiransomware;
- segnalare immediatamente al reparto IT il malfunzionamento dei beni consortili;
- attivare manualmente, prima di assentarsi dal proprio posto di lavoro, l'utente è tenuto ad il blocco del personal computer seguendo queste istruzioni: cliccare contemporaneamente i tasti CTRL-ALT-CANC (DEL per i portatili), quindi cliccare sul pulsante "blocca computer"; per sbloccare il computer sarà necessario utilizzare la password dell'utente;
- inviare, ricevere, conservare SMS, whatsapp, MMS per fini personali e/O offensivi e/o discriminatori;
- utilizzare un "codice di blocco" per prevenire l'uso improprio dei telefoni cellulari consortili assegnati, con un PIN il più lungo possibile, in uso e l'accesso ai dati in esso contenuti;
- utilizzare gli apparati per scattare fotografie personali, registrare filmati, scaricare musica e giochi.

Co.va.r 14 procederà, ogni anno alla fine del mese di aprile, previa comunicazione ad hoc il 30 di marzo, ad ordinare la cancellazione dei dati personali conservati sui beni consortili, in uso ad ogni dipendente, che non siano stati precedentemente cancellati.

2.PROCEDURE VIETATE

- concedere il proprio elaboratore portatile, tablet, smartphone in uso a terzi
- configurare mail consortili su dispositivi personali

3. DISATTIVAZIONE O CESSAZIONE DEL RAPPORTO DI LAVORO

L'ente si riserva la facoltà di disabilitare l'utilizzo dei mezzi sopra elencati resi disponibili. Tali mezzi, infatti, sono strumenti consortili messi a disposizione del dipendente/collaboratore al fine di consentirgli lo svolgimento della propria mansione ma, come tutti gli strumenti di lavoro, essi rimangono nella completa e totale disponibilità dell'ente.

In caso di disattivazione o di cessazione del rapporto di lavoro gli strumenti vanno riconsegnati al Titolare del trattamento/Ufficio IT

Al momento della restituzione dei beni o entro 15 giorni dalla restituzione, l'ente invita l'interessato (ex dipendente) ad estrarre dai beni consortili ogni possibile dato personale. L'ente mediante un soggetto autorizzato, redige apposito verbale sull'attività realizzata. Il verbale va sottoscritto anche dall'ex dipendente.

Concluso il suddetto termine, tutti i beni contenuti in supporti consortili verranno considerati dati consortili.

***

In caso di cambiamenti di unità organizzative o, in ogni caso, di trasferimenti dei dipendenti, le eventuali risorse ICT ad essi precedentemente assegnate sono sottoposte nuovamente a processo autorizzativo

8.6 PERIFERICHE DI MASSA (USB PEN-DRIVE)

1. PROCEDURE CORRETTE

- utilizzare solo periferiche di archiviazione di massa richieste al reparto IT;
- proteggere le periferiche tramite PIN minimo di 8 caratteri;
- non comunicare il PIN a terzi;
- formattare la periferica prima di riconsegnarla
- riconsegnare la/le periferiche all'IT al termine del loro utilizzo.

2. PROCEDURE VIETATE

- utilizzare periferiche di archiviazione di massa private e non richieste all'IT;
- comunicare il PIN a terzi;

Tutte le periferiche di archiviazione di massa dovranno essere censite ed i relativi PIN, o chiavi di ripristino, saranno custoditi all'interno di un file/directory protetto/a da password conservato dal responsabile IT, in modo tale da risalire al soggetto affidatario della periferica di massa.

Ad ogni cambio utente dovrà essere cambiato il PIN, o chiave di ripristino o password, con conseguente formattazione della periferica stessa.

9 PROTEZIONE FIREWALL, ANTIVIRUS, ANTIMALWARE, ANTIRANSOMWARE

1. PROCEDURE CORRETTE

- tenere sempre attivati ed aggiornati i software firewall, antivirus, antimalware, antiransomware installati sul pc ;
- avvisare immediatamente l'Ufficio IT in ogni caso di anomalia;
- segnalare all'Ufficio IT il distacco dalla rete consortile del portatile per un periodo superiore a 15 giorni;
- seguire le istruzioni specificatamente indicate in caso di avviso da parte del software antimalware, in particolare, in caso di minaccia rilevata come non risolvibile procedere a:
    - disconnettere il cavo di rete e di alimentazione e nel caso di PC portatile o palmare spegnerlo;
    - contattare Direzione IT.

***

In ogni caso è responsabilità della Direzione IT mantenere aggiornato il software antimalware, generalmente attraverso un processo automatizzato mentre l'utente è connesso alle risorse di rete.

2. PROCEDURE VIETATE

- Disabilitare o eludere il software antimalware antivirus sulla propria postazione.

10 INTERNET

1. PROCEDURE CORRETTE

- utilizzare la rete internet dalle 13.00 alle 14.00;

2. PROCEDURE VIETATE

- navigare su siti illeciti, contrari alla morale e/o discriminatori per sesso e razza.
- utilizzare social network, webchat salvo specifica autorizzazione della Direzione

11 POSTA ELETTRONICA

1. PROCEDURE CORRETTE

- utilizzare la mail per fini personali durante la pausa pranzo dalle ore 13.00 alle ore 14.00;
- modificare la password almeno ogni 90 giorni ed immediatamente qualora si sospetti che essa sia venuta a conoscenza di terzi;
- gestire la casella di posta elettronica, la cui dimensione è stabilita in funzione delle necessità operative, in modo opportuno, eliminando i messaggi personali non necessari all'attività lavorativa, contenendo la dimensione degli stessi e dei relativi allegati. Ciò al fine di conseguire un più efficace impiego del servizio di posta elettronica, e nel contempo non sovraccaricare i relativi sistemi di sicurezza;
- cancellare immediatamente la mail in caso di messaggi sconosciuti o insoliti;
- memorizzare solo le email necessarie alla propria attività;
- utilizzare sempre i formati compressi (zip, rar etc) per inviare allegati pesanti

***

Co.va.r 14 procederà, ogni anno nel mese di aprile, previa comunicazione ad hoc il 30 di marzo, ad ordinare la cancellazione delle mail personali conservate sull'indirizzo di posta elettronica consortile, in uso ad ogni dipendente, che non siano state precedentemente cancellate.

Al termine di tale periodo le suddette mail verranno, in ogni caso, considerate mail consortili.

Le mail consortili verranno conservate 10 anni per finalità amministrative, contabili e gestionali.

2 PROCEDURE VIETATE

- utilizzare la posta elettronica per inviare a terzi documenti di lavoro o file strettamente riservati;
- partecipare o continuare catene telematiche (es Catene di sant'antonio)
- inviare o memorizzare messaggi il cui contenuto sia illegale, oltraggioso o osceno ovvero possa costituire o incitare alla discriminazione per ragioni di sesso, razza, lingua, religione, origine etnica, opinioni ed appartenenza sindacale e/o politica;
- inviare documenti consortili se non nei limiti delle proprie mansioni, responsabilità ed esigenze di progetto;
- aprire messaggi di posta elettronica o allegati di tipo "eseguibile" (formato " . exe") salvo in caso di certezza assoluta del mittente;
- partecipare, salvo autorizzazione del proprio responsabile, a dibattiti, forum, mailing-list, ecc., attivate esternamente all'ente;
- usare false identità durante lo scambio di messaggi;
- rispondere o aprire link contenuti in messaggi di posta che:
    - contengono un messaggio generico di richiesta di informazioni personali per motivi non ben specificati (ad es. scadenza, smarrimento, problemi tecnici);
    - fanno uso di toni intimidatori‖, quali ad esempio la minaccia del blocco della carta di credito o del conto corrente in caso di mancata risposta dell'utente. Le banche e gli istituti di credito, infatti, non richiedono mai per posta elettronica informazioni attinenti il conto personale o depositi. Le suddette precauzioni hanno lo scopo di evitare che sia rubata l'identità e che siano eseguite operazioni ad insaputa dell'utente vittima.

3.PROCEDURE IN CASO DI ASSENZA

In caso di assenza programmata (ad esempio per ferie o attività di lavoro fuori sede che pregiudichino la visibilità della posta elettronica) è opportuno impostare all'interno di client di posta elettronica o facendo richiesta all'IT messaggi di risposta automatici per permettere ai mittenti delle mail di essere consapevoli dell'assenza dall'ente nonché di ricevere indicazioni in merito a possibili referenti alternativi.

In ogni caso qualora l'ente al fine di perseguire finalità strettamente consortili dovesse avere necessità di accedere alla posta consortile del soggetto assente si segue la procedura per le assenze improvvise.

Qualora, in caso di assenza improvvisa e/o prolungata, ricorrano improrogabili necessità legate all'attività lavorativa per cui si debba conoscere il contenuto dei messaggi di posta elettronica, il Responsabile di Funzione/Direzione di appartenenza dell'utente può richiedere all'Amministratore di sistema che venga effettuato il reset della password dell'utente stesso. Di tale attività deve essere redatto, a cura del suddetto Responsabile, apposito verbale e deve essere informato l'utente interessato, preventivamente o, ove ciò non sia possibile, alla prima occasione utile.

In ogni caso, l'ente al fine di perseguire le finalità strettamente consortili ha previsto un sistema di delega.

In particolare ciascun dipendente può nominare un fiduciario anche tramite la funzionalità della casella di posta " accesso e delega", in caso di attivazione.

12 CESSAZIONE DEL RAPPORTO DI LAVORO

In caso di licenziamento o dimissioni del dipendente l'ente provvede alla disattivazione (chiusura) dell'account consortile riferita all'ex dipendente entro 15 giorni dalla data del licenziamento o delle dimissioni.

Contestualmente l'amministratore di sistema attiva un risponditore automatico volto a comunicare la chiusura dell'account dell'ex dipendente durante 15 giorni e ad invitare il mittente a ri-inviare la mail ad altro soggetto specificatamente individuato.

Durante il suddetto periodo temporale, ossia 15 giorni, l'ente in contraddittorio con altro soggetto dell'ufficio di appartenenza dell'ex dipendente, potrà verificare nella mail consortile dell'ex dipendente l'eventuale presenza di email ed, in tal caso, potrà constatare il solo nominativo del mittente, senza aprire alcuna mail, al fine di poterlo contattare in per finalità consortili.

Nell'arco dei 15 giorni l'ente invita l'interessato (ex dipendente) ad estrarre dalla posta elettronica ogni possibile dato personale. L'ente mediante un soggetto autorizzato, redige apposito verbale sull'attività realizzata. Il verbale va sottoscritto anche dall'ex dipendente.

Al termine dei 15 giorni la mail dell'ex dipendente va completamente disattivata ossia chiusa.

13 TELEFONI FISSI, FAX, STAMPANTI E FOTOCOPIATRICI

1. PROCEDURE CONSENTITE

- l'uso privato, purché occasionale, non prolungato e limitato alle situazioni di effettiva necessità, degli apparati di telefonia fissa e cellulare assegnati in uso;
- cancellare, nel caso in cui gli apparati debbano essere restituiti o inviati in manutenzione, dalle memorie degli apparati stessi qualsiasi dato personale proprio o di soggetti terzi.
- ritirare prontamente la stampa dai vassoi delle stampanti / fotocopiatori comuni.
- archiviare in apposita cartella il documento precedentemente scansionato e procedere a cancellare la mail

2. PROCEDURE VIETATE

- effettuare o ricevere telefonate personali e comunque non attinenti ai compiti affidati;
- comunicare i numeri telefonici a call center, società di servizi di informazione o di intrattenimento in abbonamento via SMS, comunità virtuali, ecc;
- l'uso di fax, stampanti e fotocopiatori per fini personali;
- utilizzare, in ogni caso, gli apparati per attività non pertinenti con lo svolgimento delle mansioni affidate.

14 ACCESSO AI DATI TRATTATI – AMMINISTATORE DI SISTEMA O SUO DELEGATO

Il personale incaricato alla gestione tecnica degli strumenti informatici può:

a) accedere ai dati trattati dall'utente tramite posta elettronica, navigazione in rete per motivi di sicurezza, protezione del sistema informatico e del patrimonio consortile (ad es.,

contrasto virus, malware, intrusioni telematiche, fenomeni quali spamming, phishing, spyware, ecc.), ovvero per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa e/o su segnalazione di presunti comportamenti illeciti. Fatta eccezione per gli interventi urgenti che si rendano necessari per affrontare situazioni di emergenza e sicurezza, il personale incaricato accederà ai dati su richiesta dell'utente e/o previo avviso al medesimo. Ove sia necessario per garantire la sicurezza, l'assistenza tecnica e la continuità della normale attività operativa, il personale incaricato avrà anche la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni;

b) nei casi indicati alla lett. a) che precede, effettuare tutte le operazioni di configurazione e gestione necessarie a garantire la corretta funzionalità del sistema informatico consortile (ad es. rimozione di file o applicazioni pericolose);

c) procedere a controlli finalizzati a garantire l'operatività e la sicurezza del sistema, nonché il necessario svolgimento delle attività lavorative, es. mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. L'eventuale controllo sui file di log da parte del personale incaricato alla gestione tecnica degli strumenti informatici non è comunque continuativo ed è limitato:
   - per la posta elettronica all'indirizzo del mittente e del destinatario, alla data e all'ora dell'invio e della ricezione e all'oggetto;
   - per la navigazione in internet al nome dell'utente, all'identificativo della postazione di lavoro (indirizzo IP), alla data e ora di navigazione, al sito visitato e al totale degli accessi effettuati;

d) può accedere ai dati contenuti negli strumenti informatici restituiti dall'utente all'ente per cessazione del rapporto, sostituzione delle apparecchiature, ecc. Sarà cura dell'utente la cancellazione preventiva di tutti i dati personali eventualmente ivi contenuti.

In ogni caso, l'ente effettua trattamenti tecnicamente finalizzati a consentire il regolare e corretto svolgimento dei servizi e-mail e internet anche ai fini connessi al rapporto di lavoro.

15 POSSIBILITA' DI CONTROLLI E LORO GRADUALITA'

Al fine di prevenire le succitate criticità e rischi, l'ente si riserva la facoltà di effettuare rilevazioni, in forma aggregata e anonima, in merito alla corretta applicazione dei principi e delle regole consortili.

Le modalità di svolgimento delle sopraindicate rilevazioni garantiranno il rispetto dei principi di pertinenza e non eccedenza, evitando qualunque immotivato accesso a dati personali contenuti nelle risorse informatiche consortili.

In caso di anomalie riscontrate nell'utilizzo delle risorse informatiche, la competente unità della funzione ICT effettua le operazioni necessarie ad identificare la causa del problema in esame.

In ogni caso saranno effettuati controlli graduali: in via preliminare, sempre in forma aggregata e anonima, sui dati relativi all'utilizzo delle risorse informatiche consortili riferiti a gruppi di lavoro.

Le rilevazioni verranno effettuate in maniera tale da salvaguardare l'anonimato, saranno oggetto di un reporting ai Privacy Officer circa le anomalie rilevate relativamente al corretto utilizzo delle risorse informatiche consortili.

Qualora le predette rilevazioni mostrino anomalie nell'utilizzo delle risorse informatiche, il Privacy Officer di riferimento invia a tutti i propri collaboratori un avviso che inviti loro ad attenersi alle regole di comportamento per l'utilizzo delle risorse informatiche consortili, fermo restando l'eventuale successivo approfondimento delle verifiche e, ove necessario, l'accertamento di **responsabilità individuali.**

In ogni caso, non saranno effettuati controlli prolungati, costanti od indiscriminati.

I dati sull'utilizzo di internet e della posta elettronica consortile sono registrati e archiviati in banche dati informatiche a cura della competente unità della funzione ICT. La gestione e la sicurezza delle banche dati è realizzata in conformità alle disposizioni vigenti in materia di tutela dei dati personali. I relativi trattamenti, sono eseguiti da personale incaricato. Il Titolare del trattamento è Co.va.r 14.

I dati registrati sono conservati per il tempo strettamente necessario al perseguimento delle finalità per le quali sono stati registrati e comunque per un periodo non superiore a 12 mesi, trascorsi i quali si procede alla relativa cancellazione, fatti salvi in ogni caso specifici obblighi di legge (ad es. Richiesta dell'Autorità Giudiziaria) o specifiche necessità di tutela e difesa degli interessi consortili.

I dati personali di un singolo dipendente, eventualmente anche sensibili, ricavabili dai dati registrati sono trattati, nei limiti in cui ciò sia indispensabile, per un periodo di tempo anche superiore, comunque non eccedente alle finalità, in caso di:

- richiesta scritta, ordinanza, decreto o altro provvedimento da parte della magistratura, del Garante per la Protezione dei Dati Personali o delle Forze dell'Ordine o altra Authority, nell'ambito dell'esercizio delle loro funzioni istituzionali;

- azioni legali avanzate nei confronti dell'ente da parte di terzi che ritenessero violati i propri diritti in materia di privacy;
- presunzione di comportamenti illeciti o rilevanti violazioni di Regolamenti consortili e/o obblighi.

In tali casi, in relazione alle specifiche casistiche di propria competenza, le competenti unità nell'ambito delle funzioni legale e risorse umane (rispettivamente per le tematiche di natura civile o penale e per le tematiche giuslavoristiche) nel valutare le azioni da intraprendere, individueranno anche gli eventuali dati da reperire:

- d'intesa con il Competente Privacy Officer;
- nel rispetto delle disposizioni di legge applicabili;
- tenendo in considerazione la complessità, onerosità e fattibilità tecnica delle attività da compiersi ai fini del loro reperimento in relazione anche alla natura e provenienza della richiesta.

La richiesta è quindi inoltrata alla competente unità della funzione ICT.

16 CASI DI INOTTEMPERANZA

Il rispetto delle prescrizioni contenute nella presente normativa costituisce parte essenziale delle obbligazioni contrattuali alle quali gli utenti devono attenersi secondo la diligenza richiesta nello svolgimento dell'attività lavorativa.

L'eventuale utilizzo improprio delle risorse informatiche consortili rappresenta violazione degli obblighi derivanti dal rapporto di lavoro e, conseguentemente, illecito disciplinare perseguibile secondo quanto previsto dal CCNL applicabile.

Per l'utilizzo dei dati tracciati con gli strumenti di cui al presente regolamento a tutti i fini connessi al rapporto di lavoro si rinvia altresì alla specifica informativa effettuata ai sensi dell'art. 4, comma 3, della legge n. 300 del 1970 che si considera parte integrante del presente Regolamento.

Data *Firma*

_____ _____

CONSORZIO COVAR 14

MODELLO ORGANIZZATIVO PRIVACY IN CONFORMITÀ AL CODICE PER LA PRIVACY D.LGS 196/2003 AGGIORNATO AL DECRETO ARMONIZZAZIONE ED AL REGOLAMENTO EUROPEO UE N. 2016/679 SULLA PROTEZIONE DEI DATI PERSONALI

Identificazione del documento

Codice:	MOP.2019	
Titolo:	Modello Organizzativo Privacy	

Stato delle edizioni

Edizione n°	**Motivo della edizione**	**Data**
1	Prima emissione	.2019

Approvazione ed emissione

	Data	**Firma**
Verificato ed approvato: (rappresentante legale o Cda)		

Indice

1. Finalità e ambito d'applicazione ..... Errore. Il segnalibro non è definito.

1.1 Finalità ..... **Errore. Il segnalibro non è definito.**
1.1.1 Definizioni ..... **Errore. Il segnalibro non è definito.**
1.2 Ambito d'applicazione delle presenti direttive .... **Errore. Il segnalibro non è definito.**
1.3 Principi Privacy ..... **Errore. Il segnalibro non è definito.**
1.3.1 Principio di Accountability ..... **Errore. Il segnalibro non è definito.**
1.3.2 Principi By Design e By Default ..... **Errore. Il segnalibro non è definito.**
1.4 Modifiche rispetto alla edizione precedente ..... **Errore. Il segnalibro non è definito.**
1.5 Riferimenti normativi e documentali ..... **Errore. Il segnalibro non è definito.**
1.6 Variazioni organizzative e tecniche che possono avere impatto sui trattamenti .. **Errore. Il segnalibro non è definito.**

2. Trattamenti di dati personali ..... Errore. Il segnalibro non è definito.

Premessa

2.1. Rapporti tra Covar 14, Pegaso 03 Srl e Comuni 10
2.2. Finalità del trattamento 10
2.3 Elenco dei trattamenti nell'ambito di attività ..... **Errore. Il segnalibro non è definito.**
2.3.1 Il Registro dei Trattamenti ex art 30 GDPR ..... **Errore. Il segnalibro non è definito.**
2.3.2 Il contenuto dei registri ..... **Errore. Il segnalibro non è definito.**
2.3.3 Categorie particolari di Interessati verificare ..... **Errore. Il segnalibro non è definito.**
2.3.4 Trattamenti dati giudiziari ex art. 10 GDPR VERIFICARE **Errore. Il segnalibro non è definito.**
2.3.5 Trattamenti in conformità alla normativa in materia di trasparenza VERIFICARE **Errore. Il segnalibro non è definito.**

3. ORGANIGRAMMA PRIVACY **16**

3.1.Titolare del trattamento ..... **Errore. Il segnalibro non è definito.**
3.2 Contitolare ..... **Errore. Il segnalibro non è definito.**
3.3 Data Profection Officer ..... **Errore. Il segnalibro non è definito.**
3.4Persone autorizzate al trattamento ..... **Errore. Il segnalibro non è definito.**
3.5 Data Manager e Privacy Officer ..... **Errore. Il segnalibro non è definito.**
3.6 Privacy Offier it ..... **Errore. Il segnalibro non è definito.**

4. RESPONSABILI ESTERNI ..... Errore. Il segnalibro non è definito.

4.1 COVAR 14 nomina responsabili esterni del trattamento 25
4.2 COVAR 14 nomina Subresponsabili del trattamento **Errore. Il segnalibro non è definito.**
4.2 COVAR 14 in qualità Responsabile Esterno .....
4.4 COVAR 14 in qualità di subresponsabile

5. PROFESSIONISTI ESTERNI CHE TRATTANO DATI PER CONTO D SCRP . Errore. Il segnalibro non è definito.

6. SITO INTERNET ..... Errore. Il segnalibro non è definito.

7. DIRITTI DEGLI INTERESSATI ..... Errore. Il segnalibro non è definito.

7.1 Diritto di accesso ex art. 15 GDPR ..... **Errore. Il segnalibro non è definito.**
7.2. Diritto di rettifica ex art. 16 GDPR ..... **Errore. Il segnalibro non è definito.**
7.3. Diritto all'oblio ex art. 17 GDPR ..... **Errore. Il segnalibro non è definito.**

7.4. Diritto alla limitazione del trattamento ex art. 18 GDPR ..... **Errore. Il segnalibro non è definito.**
7.5. Diritto alla portabilità ex art. 20 GDPR ..... **Errore. Il segnalibro non è definito.**
7.6. Diritto di opposizione ex art. 21 GDPR ..... **Errore. Il segnalibro non è definito.**
7.7. Processo decisionale automatizzato relativo alle persone fisiche compresa la profilazione ex art. 22GDPR ..... **Errore. Il segnalibro non è definito.**
7.8 Informativa e consenso ..... **Errore. Il segnalibro non è definito.**
7.8.1 Informativa ..... **Errore. Il segnalibro non è definito.**
7.8.2 Consenso 35
8. SICUREZZA DEI TRATTAMENTI E RIPRISTINO DEI DATI Errore. Il segnalibro non è definito.
8.1 Fonti di pericolo ..... **Errore. Il segnalibro non è definito.**
8.1.2 Misure tecniche ed organizzative ..... **Errore. Il segnalibro non è definito.**
8.2 Premessa IT 39
8.2.1 Analisi dei rischi 39
8.2.2 Analisi fisica della struttura 40
8.2.3. Asset aziendali 41
8.2.4 Elenco dei database 42
8.2.5 Utenze e accessi ai database 43
8.2.6 Misure logiche di sicurezza 44
8.2.7 Criteri e modalità di ripristino dei dati 52
8.2.8 Criteri di dismissione/riutilizzo hardware 53
8.2.9 Sistema di report 53
8.3 Valutazione Impatto del rischio ..... **Errore. Il segnalibro non è definito.**
8.3.1 Soggetti coinvolti ..... **Errore. Il segnalibro non è definito.**
8.3.2 Tempi e casi in cui è prevista la DPIA ..... **Errore. Il segnalibro non è definito.**
8.3.3 Consultazione ..... **Errore. Il segnalibro non è definito.**
8.3.4 Contenuto della valutazione ..... **Errore. Il segnalibro non è definito.**
8.3.5 La consultazione preventiva ed il suo contenuto **Errore. Il segnalibro non è definito.**
9. Data Breach ..... Errore. Il segnalibro non è definito.
9.1 Notificazione all'autorità di controllo ..... **Errore. Il segnalibro non è definito.**
9.2 Notificazione all'interessato ..... **Errore. Il segnalibro non è definito.**
10. MISURE DI CONTROLLO ..... Errore. Il segnalibro non è definito.
10.1 Misure edilizie ..... **Errore. Il segnalibro non è definito.**
10.1.1 Accesso ai locali ..... **Errore. Il segnalibro non è definito.**
10.2 Integrazione col sistema di Gestione ..... **Errore. Il segnalibro non è definito.**
10.3 Applicazione normativa D.lgs 81/2008 ..... **Errore. Il segnalibro non è definito.**
10.4 Videosorveglianza ..... **Errore. Il segnalibro non è definito.**
10.4.1 Interessati ..... **Errore. Il segnalibro non è definito.**
11. Misure per il personale ..... Errore. Il segnalibro non è definito.
11.1 Procedura di selezione ed ingresso dei collaboratori ..... **Errore. Il segnalibro non è definito.**
11.1.1 Consegna documentazione privacy dipendenti . **Errore. Il segnalibro non è definito.**
11.2. Regolamento aziendale ..... **Errore. Il segnalibro non è definito.**
11.3 Formazione ..... **Errore. Il segnalibro non è definito.**
11.3.1 Formazione iniziale ..... **Errore. Il segnalibro non è definito.**
11.3.2 Formazione continua ..... **Errore. Il segnalibro non è definito.**
11.4 Procedura di dimissione ..... **Errore. Il segnalibro non è definito.**
12 Data Retention ..... Errore. Il segnalibro non è definito.

12.1 Policy Data Retention .....**Errore. Il segnalibro non è definito.**
APPENDICE 1..... Errore. Il segnalibro non è definito.
Terminologia.....**Errore. Il segnalibro non è definito.**
1. Terminologia afferente al Regolamento Europeo 679/2016..... **Errore. Il segnalibro non è definito.**
2. Terminologia afferente al sistema informatico **Errore. Il segnalibro non è definito.**

1. Finalità e ambito d'applicazione

1.1 Finalità

Il presente documento rappresenta il Modello Organizzativo Privacy (MOP) ed ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione in virtù del: Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "RGPD", Regolamento Generale Protezione Dati), Codice per la privacy (D.lgs 196/2003) relativi alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati all'interno di **COVAR 14**.

Si è in attesa dell'atto di Governo.

Con l'osservanza di questo modello s'intende richiamare tutte le risorse operanti all'interno di **COVAR 14** rispetto della normativa sulla sicurezza dei dati personali, con espressa attenzione all'impiego delle risorse informatiche.

Deve essere aggiornato in relazione alla evoluzione del settore e del contesto ed almeno annualmente; la redazione e aggiornamento deve essere approvato con delibera dell'Organo amministrativo.

Nel caso in cui subentrino nel corso dell'anno modifiche che implichino ulteriori revisioni del MOP, queste devono essere predisposte in tempi rapidi e senza indebiti ritardi.

Le modalità di approvazione, gestione e diffusione del MOP sono sotto la responsabilità del Titolare del trattamento.

Il presente documento rappresenta la procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche organizzative al fine di garantire la sicurezza del trattamento ex art. 32 paragrafo 1, lett. d).

1.1.1 Definizioni

Oltre alle definizioni di cui all'art. 4 del GRDP e art. 4 del D.lgs 196/2003, valgono le seguenti:

- Privacy officer– funzioni incaricate di supportare il Titolare del trattamento e gli autorizzati nella gestione operativa della privacy in **COVAR 14.**
- Autorizzati – funzioni incaricate di trattare i dati personali degli interessati

1.2 Ambito d'applicazione delle presenti direttive

Questo documento è vincolante sia per gli autorizzati di **COVAR 14** sia per i dipendenti con altre forme di contratto e/o collaborazione, operanti in sede per i Responsabili del trattamento e per le parti applicabili.

1.3 Principi Privacy

1.3.1 Principio di Accountability

Il Regolamento europeo N 976/16 prevede tra i suoi architravi il **principio di responsabilizzazione** ("accountability") così come elencati all'articolo 5, Capo II del Regolamento.

Tale principio, non espressamente previsto dalla Direttiva, era stato oggetto di analisi specifica da parte del Gruppo di Lavoro ex articolo 29 ("Garante Europeo") nel parere n.3/2010, con il quale il Garante Europeo, già in allora ,rilevava **la necessità che il trattamento dei dati personali all'interno dell'Unione Europea fosse ispirato e guidato da un generale principio di responsabilità**, inteso come motore di attuazione di tutti gli altri principi su cui si fonda la tutela dei dati personali.

L'articolo 5, al paragrafo 2 introduce il principio di responsabilizzazione: "**il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo**".

Pur risultando complesso definire cosa si intenda per "accountability", in generale viene posto l'accento sulla "dimostrazione di come viene esercitata la responsabilità e sulla sua verificabilità. La responsabilità e l'obbligo di rendere conto (circa la conformità delle pratiche al regolamento sono due facce della stessa medaglia ed entrambe sono elementi essenziali di una buona governance. Solo quando si dimostra che la

responsabilità funziona effettivamente nella pratica può instaurarsi una fiducia sufficiente" [1]".

In sostanza, tale principio si incentra su 3 elementi principali:

1) La necessità di adottare politiche e misure adeguate per attuare i principi di protezione dei dati;

2) La necessità di dimostrare, su richiesta, che sono state adottate misure appropriate ed efficaci (**acquisizione di evidenze probatorie finalizzate a comprovare che le disposizioni del Regolamento siano state rispettate)**;

3) La "trasparenza" intesa come garanzia della completa accessibilità alle informazioni, in primo luogo per i cittadini, anche in quanto utenti del servizio.

Il Regolamento suggerisce alcune modalità mediante le quali dare attuazione al **principio di responsabilizzazione,** in particolare:

- Codici di condotta e certificazioni ex art 40 e 42;

- Tenuta di registri. In proposito il considerando 82 prevede che il titolare del trattamento o il responsabile del trattamento "per dimostrare che si conforma al presente regolamento – in attuazione del suddetto principio – dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità". Fatta salva, infatti, l'obbligatorietà della tenuta dei registri dei trattamenti soltanto per i titolari che soddisfino le condizioni di cui all'articolo 30 del Regolamento, il sopracitato considerando prosegue "Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per monitorare detti trattamenti";

- I "data breach" – inteso come obbligo di comunicazione dell'avvenuta violazione di dati personali;

- il Data Protection Officer ("DPO") anche per esso sono previsti casi obbligatori.

In ogni caso "**nonostante l'applicazione obbligatoria di tali istituti sia prevista solo in alcune ipotesi tassative, la relativa disciplina dovrebbe ispirare tutti i titolari dei trattamenti all'adozione di condotte "responsabili e coscienti"**, basate su una **valutazione preliminare** dei rischi derivanti dal trattamento e

[1] Parere 3/10 WP29

sull'adeguatezza delle misure da adottare e, in generale, su una forte consapevolezza dell'importanza della normativa sulla protezione dei dati personali"[2].

1.3.2 Principi By Design e By Default

L'art. 25 del Regolamento europeo prevede espressamente i principi di by design e by default. In particolare, con il termine By design si intende che la protezione dei dati deve avvenire sin dalla progettazione e quindi prima che avvenga il trattamento.
Il considerando n. 78 statuisce che "La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. **Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default.** Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza.
Alla base del concetto di privacy by design vi sono i seguenti principi:

- prevenire non correggere, cioè i problemi vanno valutati nella fase di progettazione;
- privacy come impostazione di default;
- privacy incorporata nel progetto;
- massima funzionalità, in maniera da rispettare tutte le esigenze (rifiutando le false dicotomie quali più privacy = meno sicurezza);
- sicurezza durante tutto il ciclo del prodotto o servizio;
- trasparenza;

[2] Guida II al Regolamento Privacy UE 2016/679: i principi generali del trattamento e l'accountability o responsabilizzazione 23 maggio 2017 Marco Dettori, Iusgate

- centralità dell'utente.

Per quanto riguarda l'aspetto complementare ossia privacy By default previsto dal comma 2 dell'art 25, esso sta a significare che la tutela della protezione del dato deve diventare per "impostazione predefinita".
Tale principio stabilisce che per impostazione predefinita le imprese dovrebbero trattare solo i dati personali nella misura necessaria per le finalità previste e per il periodo strettamente necessario a tali fini.
Va osservato che anche gli incaricati del trattamento e i produttori devono attuare le misure e le procedure tecniche e operative adeguate per garantire che i loro servizi e prodotti consentano ai responsabili del trattamento, di default, di conformarsi al presente Regolamento.

1.4 Modifiche rispetto alla edizione precedente

Il MOP è alla prima emissione. **COVAR 14** ha deciso di controllare, tramite l'aggiornamento del MOP medesimo gli aspetti relativi all'applicazione del Regolamento Europeo Privacy a maggiore garanzia delle attività svolte e dei controlli effettuati.

1.5 Riferimenti normativi e documentali

- Regolamento Europeo Ue n. 679/2016 sulla protezione dei dati personali.
- Linee Guida del Gruppo 29 in merito al Responsabile sulla protezione dei dati;
- Linee guida sulla valutazione d'impatto e successive integrazioni;
- Linee Guida del Gruppo 29 in merito all'individuazione dell'autorità capofila;
- Linee Guida in materia di data breach notification nonchè sulla profilazione.
- Vademecum del Garante sull'attività di recupero crediti del 2016 ove ha ripreso un Provvedimento emanato nel 2005;
- Provvedimento prescrittivo in materia di biometria del 2014;
- Provvedimento prescrittivo in materia di geolocalizzazione del 2011;
- Provvedimento in materia di videosorveglianza del 2011;
- Provvedimento del 2008 in materia di amministratore di sistema e successive integrazioni del 30 giugno 2009;

- Linee Guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati approvata con deliberazione n. 53 del 23 novembre 2006;
- Racc. 5/15
- Opinion 2/17 Wp29
- Linee Guida del Garante per posta elettronica ed internet Deliberazione n. 58 del 10 marzo 2007
- Linee Guida sul consenso del 18.1.18
- Codice per la protezione dei dati D.lgs 196/2003
- Decreto di armonizzazione, ad oggi in attesa di essere emesso
- Provvedimenti emessi dal Garante del Privacy
- Decreto armonizzazione n. 101/2018

1.6 Variazioni organizzative e tecniche che possono avere impatto sui trattamenti

Poiché la presente è la prima versione del documento e non sono ancora state apportate variazioni organizzative e tecniche quali ad esempio, nuovi responsabili esterni del trattamento, nuovi trattamenti, nuovi sistemi informatici, operazioni straordinarie di impresa (es. fusioni, cessioni, trasformazioni, ecc.), tale paragrafo non è attualmente applicabile.

2. Trattamenti di dati personali

Premessa

2.1 Rapporti tra Covar 14, Pegaso 03 Srl e Comuni

Co.Va.R. 14 è il Consorzio obbligatorio di bacino, previsto dalla legge regionale 24/2002 e costituito ai sensi del decreto legislativo 267/2000, che esercita le funzioni di governo e coordinamento dell'organizzazione dei servizi di bacino per assicurare la gestione unitaria dei rifiuti urbani nella fase di raccolta, avvio a recupero e smaltimento.
Fanno parte del Co.Va.R. 14 i Comuni di: Beinasco, Bruino, Candiolo, Carignano, Castagnole Piemonte, La Loggia, Lombriasco, Moncalieri, Nichelino, Orbassano, Osasio, Pancalieri, Piobesi Torinese, Piossasco, Rivalta Torinese, Trofarello, Villastellone, Vinovo e Virle Piemonte.
La Convenzione tra il Consorzio ed i suddetti Comuni specifica che " *il Consorzio persegue le finalità di tutela della salute dei cittadini, di difesa dell'ambiente e di*

salvaguardia del territorio, nel rispetto delle vigenti normative in materia, esercita la funzione dell'ente locale titolare della proprietà degli impianti delle reti e delle altre dotazioni necessari all'esercizio dei servizi pubblici relativi ai rifiuti urbani, salvo sia costituita la società proprietaria ai sensi dell'art. 113, D.lg. 267/2000 e s.m.i.".

Lo Statuto prescrive che ciascun Ente associato partecipa ed è responsabile della gestione consortile ed esercita **l'effettiva potestà d'intervento nei processi decisionali** in sede di Assemblea consortile in misura proporzionale alla quota di partecipazione.

Sotto il profilo privacy, negli anni passati i Comuni sono stati definiti titolari del trattamento, mentre, Covar 14 responsabile del trattamento per tutte le attività che i Comuni delegano ad esso. In particolare, tale Consorzio per conto dei Comuni appalta i servizi di raccolta rifiuti e di spazzamento stradale e ne controlla la regolare esecuzione da parte delle ditte appaltatrici; controlla i flussi di rifiuti raccolti monitorandone i quantitativi e la tipologia, fino al trasporto negli impianti di recupero o di smaltimento; sottoscrive, su delega dei Comuni, le convenzioni con i consorzi di filiera del Conai per la riscossione dei contributi sui rifiuti recuperabili raccolti; progetta e affida la gestione dei centri di raccolta comunali; cura le attività di educazione ambientale e di informazione alla cittadinanza; controlla le operazioni di post conduzione delle discariche affidate in gestione e, su richiesta dei Comuni, predispone la realizzazione degli interventi di bonifica dei siti inquinati, elabora i piani finanziari, gestisce la tariffa di igiene ambientale e le segnalazioni fatte dai cittadini al Numero Verde attraverso la società Pegaso 03.

In particolare in merito alla predisposizione dei piani finanziari, essi vengono approvati dall'Assemblea consortile su proposta del Consiglio di Amministrazione osservando uno standard omogeneo per realtà territoriali analoghe, ed i singoli Comuni possono richiedere variazioni rispetto agli standards proposti giustificando tale richiesta. In merito, invece, alla tariffa di igiene ambientale, essa viene approvata dai singoli consorziati, con applicazione di coefficienti correttivi del sistema tariffario consortile in ragione delle richieste variazioni agli standards di servizio. La tariffa, quindi, è riscossa dal Consorzio previo assenso dei Comuni.

In considerazione del periodo transitorio che sta attraversando Covar 14 e che lo vede protagonista nella progettazione e creazione dell'area vasta, il Consorzio ha ritenuto, di aggiornare al Reg. Eu 16/679 i doc.ti in essere, ma di mantenere la stessa struttura

privacy già esistente, pertanto, attualmente i Comuni sono considerati per l'attività realizzata da Covar 14, titolari del trattamento.

Resta inteso, che al termine della realizzazione dell'area vasta i rapporti tra Covar 14 ed i Comuni dovranno essere rivisti alla luce sia delle finalità perseguite dal nuovo Istituto giuridico, sia in base ai soggetti che in concreto decideranno finalità e mezzi del trattamento.

2.2 Finalità del trattamento

I trattamenti sono compiuti da **COVAR 14** per le seguenti finalità:

A. esecuzione di un contratto con dipendenti e professionisti,
B. Esecuzione contratti con fornitori;
C. gestione del servizio di elaborazione della tariffa di igiene ambientale ed emissione dei relativi avvisi di pagamento;
D. predisposizione ed emissione delle bollette;
E. valutazione delle richieste degli utenti relative a pagamenti rateizzati, rimborsi, rendicontazione;
F. comunicazione, anche mediante il numero verde, di informazioni agli utenti in merito al sistema di tariffazione;
G. acquisizione domande di variazioni del nucleo familiare;
H. verifica l'iscrizione degli utenti al servizio;
I. verifica degli incassi relativi agli avvisi di pagamento e rendicontazione dell'addizionale provinciale;
J. gestione degli ecosportelli;
K. riscossione coattiva della tariffa di igiene ambientale;
L. invio informazioni riguardanti l'attività svolta da Covar 14;
M. valutazione del gradimento dei servizi;
N. Adempimento ad obblighi di legge e/o ottemperare ad ordini provenienti da pubbliche Autorità;
O. Esercizio e/o difesa di un diritto nelle sedi competenti;

2.3 Elenco dei trattamenti nell'ambito di attività COVAR 14

Nell'ambito della propria attività, **COVAR 14** tratta dati personali e dati particolari, al fine di perseguire le proprie finalità nonché quelle stabilite dai Comuni..

COVAR 14 pone la massima attenzione a che i dati siano trattati in modo lecito, corretto e sicuro, al fine di ridurre al minimo il rischio che i dati vadano distrutti o persi, anche a causa di eventi accidentali, e che persone non autorizzate li possano leggere, modificare, o utilizzare in modo improprio o diverso dallo scopo per cui sono stati raccolti.

A tal fine ha predisposto il Registro dei trattamenti sia come titolare del trattamento sia come responsabile del trattamento.

2.3.1 Il Registro dei Trattamenti ex art 30 GDPR

Il registro delle attività di trattamento dei dati personali costituisce una pietra angolare del sistema, un importante strumento di compliance aziendale in materia di dati personali.

Secondo il Garante per la protezione dei dati personali italiano "il registro dei trattamenti non costituisce un adempimento formale bensì **parte integrante di un sistema di corretta gestione dei dati personali**"[3], Lo stesso Garante privacy nella propria **Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali**[4] invita tutti i titolari del trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione a compiere i passi necessari per dotarsi di tale registro.

Il registro dei trattamenti consente alle imprese e pubbliche amministrazioni di disporre di un quadro aggiornato dei trattamenti effettuati al proprio interno e in relazioni ad altri soggetti, quadro aggiornato indispensabile per ogni valutazione e analisi del rischio.

Ai sensi delle disposizioni del regolamento privacy europeo il registro può **essere tenuto in forma scritta o anche in formato elettronico.**

Il registro dei trattamenti non costituisce un documento che una volta redatto può rimanere immutabile ma rappresenta un vero e proprio **strumento di lavoro**, e come tale deve essere modificato e deve essere mantenuto aggiornato e sempre attuale.

Tale strumento di lavoro consente all'organizzazione di disporre di un censimento dei trattamenti effettuati, delle relative finalità, degli interessati e delle categorie dei dati

[3] Garante per la protezione dei dati personali, *Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali* (http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali

[4] per la protezione Garante del dati personali, Guida all'applicazione del regolamento europeo in materia di protezione dei dati personali, giugno 2017 consultabile al link: http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali

personali, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, di una descrizione generale delle misure di sicurezza tecniche e organizzative.

La redazione dei registri dei trattamenti consente al titolare di dimostrare quali misure ha utilizzato per garantire un livello di sicurezza adeguato al rischio ed in particolare le misure adottate.

La redazione e l'aggiornamento dei registri dei trattamenti devono essere coordinati con gli altri adempimenti previsti dal regolamento privacy europeo (l'informativa privacy, la valutazione di impatto privacy, le istanze di consultazione preliminare; le comunicazioni delle violazioni di dati "data breach").

La redazione del registro dei trattamenti è stata individuata dal Garante privacy nel comunicato stampa del 14 giugno 2017 sull'impatto del regolamento europeo nel settore pubblico come una delle tre azioni ad alta priorità con la designazione del DPO e il data breach.

Si segnala come il Garante per la protezione dei dati personali francese ha già messo a disposizione on line diverso specifico materiale in materia del registro dei trattamenti tra cui anche un fac simil[5] e al fine di accompagnare le imprese e le pubbliche amministrazioni nel complesso percorso di adeguamento al regolamento privacy europeo.

2.3.2 Il contenuto dei registri

REGISTRO DEL TITOLARE	REGISTRO DEL RESPONSABILE
a)il nome e i dati di contatto del Titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del Titolare del trattamento e del Responsabile della protezione dei dati;	a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
b) le finalità del trattamento;	**No**
	b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento
c) una descrizione delle categorie di interessati e delle categorie di dati personali;	**NO**
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati,	**NO**

[5] Per approfondimenti: https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

compresi i destinatari di paesi terzi od organizzazioni internazionali	
e) ove applicabile, i trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale, compresa l'identificazione del Paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate	c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati	**NO**
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative	d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative

2.3.3 Categorie particolari di Interessati

COVAR 14 tratta dati di interessati che presentano particolari caratteristiche di vulnerabilità, quali:

- anziani;
- soggetti deboli come disoccupati e/ con situazioni economiche complesse
- altri soggetti vulnerabili e/o portatori di disabilità.

COVAR 14 svolge analisi anche nei confronti di soggetti considerati vulnerabili come da elenco sopra descritto.

I dati di soggetti vulnerabili, ad esempio portatori di disabilità, dipendenti di **COVAR 14**, sono trattati secondo quanto previsto per i dipendenti e collaboratori; particolari misure possono essere definite nell'ambito delle procedure di emergenza in ottemperanza al DLGS 81/2008; nel qual caso le informazioni necessarie per salvaguardare l'incolumità dell'interessato potranno essere comunicate all'RSPP e ai membri della squadra di emergenza.

2.3.4 Trattamenti dati giudiziari ex art. 10 GDPR

COVAR 14 non tratta atti giudiziali dei dipendenti; gli atti giudiziali trattati sono quelli relativi a:

- Amministratori;
- Organi controllo (revisori, sindaci, ecc.);
- Casellari giudiziali dei rappresentanti legali, componenti organi di controllo e di gestione, tecnici responsabili delle ditte che partecipano alle gare

Tali doc.ti sono conservati nell'ufficio del RUP competente mediante supporto cartaceo o digitale con accesso limitate al personale amministrativo.
I documenti sono conservati per 10 anni poi eliminati.

3. ORGANIGRAMMA PRIVACY

COVAR 14 ha previsto un organigramma Privacy (approvato con delibera cda n. 9 del 06 03 2019) al fine di:

- fornire, agevolmente, ogni informazione utile, in sede di controlli,
- di rendere anche i dipendenti e gli utenti informati sulle cd figure privacy in azienda
- facilitare ogni comunicazione tra gli uffici ed il DPO

3.1 Titolare del trattamento

Titolare del trattamento dei dati è COVAR 14 limitatamente ai dati dei dipendenti e del servizio di numero verde, ai dati delle newsletter.
Il titolare del trattamento è definito dall'art. 4 del Regolamento come "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" ed è disciplinato dall'art 24 del Regolamento europeo.
Nel caso di persone giuridiche pubbliche o private riconosciute o no è la persona giuridica nel suo complesso che va considerata titolare del trattamento non il singolo organo decisionale nella persona fisica o le persone fisiche che la rappresentano.
Essa, quindi, è centro di imputazione delle decisioni sulle finalità e sui mezzi di trattamento, pertanto, è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 del regolamento europeo: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
In concreto il Titolare decide:

- finalità;
- mezzi;
- nomina del responsabile;

- autorizzazione del responsabile a designare altri sub responsabili;
- nomina gli incaricati;
- nomina dei Responsabili esterni del trattamento ex art 28 RGDP;
- predisposizione dell'elenco dei Responsabili del trattamento delle strutture in cui si articola l'organizzazione di **COVAR 14**.
- sulla tenuta registro nei casi previsti dal Regolamento;
- profili di sicurezza;
- l'informativa agli interessati;
- la collaborazione con il Garante organismi di certificazioni.

Per il gruppo di lavoro 29 "Determinare le finalità ed i mezzi equivale a determinare rispettivamente il perché ed il come del trattamento [6]".

Per **mezzi** devono intendersi non solo gli strumenti come i software o hardware ma anche i profili strettamente organizzativi come il complesso di istruzioni e direttive fornite ai ruoli subalterni in merito alle modalità di trattamento dei dati.

Per **finalità** deve intendersi il motivo per il quale viene effettuato quel determinato trattamento dati personali.

La decisione in merito alle finalità è l'aspetto fondamentale che non può mai in alcun modo essere delegato.

Ai sensi dell'art. 24 del Regolamento il titolare del trattamento "mette in atto **misure tecniche ed organizzative adeguate per garantire e poter dimostrare**, che il trattamento, è effettuato conformemente al presente regolamento (esplicitazione del principio di accountability).

In primis va rilevato che per misure adeguate debba intendersi quelle misure adottate dal titolare del trattamento tenendo in considerazione "lo stato dell'arte e dei costi attuazione".

Va rilevato, in secundis, che il Regolamento non indica specificatamente quali siano le misure da adottare ma, come vedremo, ne cita alcune a titolo esemplificativo e non esaustivo. Ciò significa che la valutazione di quali misure prendere in considerazione va effettuata caso per caso in base alle finalità che si intendono perseguire.

La spiegazione di cosa il regolamento intenda per "misure tecniche" è spiegato sia nel seguente articolo, nel quale viene, tra l'altro, citato per la prima volta il principio già analizzato di "By design e By default", sia nel considerando 78.

[6] wp29 OP. 1/10 P 13

Ed invero l'art 25 del Regolamento tra le misure tecniche individua, come già anticipato, a titolo solo esemplificativo:

- La pseudonimizzazione;
- La Minimizzazione
- By design and by default
- Le misure in grado di garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi di trattamento.
- La cifratura ossia la misura di sicurezza in grado di rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi ed in tal caso il titolare non è tenuto a comunicare all'interessato la verificazione di una violazione.

Le "misure organizzative", invece, si sostanziano nelle diverse nomine che determinano una distribuzione delle responsabilità tra titolare e sottoposti. La ratio delle designazioni, è quella di consentire l'efficace applicazione delle norme.

3.2 Data Profection Officer

Occorre rilevare come il regolamento europeo individui delle ipotesi in cui la nomina è obbligatoria in particolare:

a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;

b) se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure

c) se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

Nel caso di specie COVAR 14 ha l'obbligo di nominare con delibera di CDA ai sensi dell'art 37 lett.a) del Reg. Eu 16/679 un DPO.

In proposito l'art 37 del Regolamento 679/16 specifica che il Responsabile della protezione dei dati è un professionista, che può essere sia interno sia esterno alla Società, purchè possegga conoscenze specialistiche della normativa e delle prassi in materia di protezione dati.

Ed invero egli deve, in particolare:

a) possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, della normativa e delle prassi nazionali ed europee in materia di protezione dei dati e un'approfondita conoscenza del RGPD;

b) adempiere alle sue funzioni in piena indipendenza ed in assenza di conflitti di interesse;

c) operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio.

Il DPO per peculiarità di indipendenza che lo deve contraddistinguere è preferibilmente esterno e la nomina attuale è conservata presso la Segreteria.

L'Autorità ha, inoltre, chiarito che la normativa attuale **non prevede l'obbligo per i candidati di possedere attestati formali delle competenze professionali.** Tali attestati, rilasciati anche all'esito di verifiche al termine di un ciclo di formazione, possono rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenza della disciplina ma, tuttavia, **non equivalgono a una "abilitazione" allo svolgimento del ruolo del RPD.**

La normativa attuale, tra l'altro, non prevede l'istituzione di un albo dei "Responsabili della protezione dei dati" che possa attestare i requisiti e le caratteristiche di conoscenza, abilità e competenza di chi vi è iscritto.

Si rammenta, inoltre, che i **COMPITI DEL RPD** sono:

a. **informare e consigliare il titolare o il responsabile del trattamento**, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento europeo e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b. **verificare l'attuazione e l'applicazione del Regolamento,** delle altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati
c. fornire, se richiesto, **pareri in merito alla valutazione d'impatto** sulla protezione dei dati e sorvegliare i relativi adempimenti;
d. **fungere da punto di contatto per gli interessati** in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti;
e. **fungere da punto di contatto per il Garante** per la protezione dei dati personali oppure, eventualmente, consultare il Garante di propria iniziativa.

Il Gruppo di lavoro 29 (insieme dei garanti europei) ritiene che rientrino tra i compiti di controllo svolti dal RPD:

- la raccolta di informazioni per individuare i trattamenti svolti;
- l'analisi e la verifica dei trattamenti in termini di loro conformità,
- l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile.

La funzione riceve autorità dall'Organo di Governo.

I principali compiti del RPD nei confronti di **COVAR 14**, in relazione agli aspetti relativi all'applicazione del Regolamento Privacy sono:

- verificare l'attuazione e l'applicazione del Regolamento sia una volta ultimato l'adeguamento da parte dell'ente sia a fronte di aggiornamenti normativi e/o giurisprudenziali
- informare e consigliare il titolare del trattamento, nonché lo staff dirigenziale e/o i dipendenti in merito agli obblighi derivanti dal Regolamento europeo e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- tenere i rapporti con il Garante ed effettuare le notifiche e le comunicazioni previste dalla legge.

La funzione fornisce al Titolare del trattamento elementi di valutazione sull'applicazione della norma (valutazione del rischio, registro per il trattamento dei dati personali, valutazioni di impatto del rischio) contribuendo all'adeguamento delle disposizioni, in relazione agli aggiornamenti di legge.

Il RPD inoltre deve:

- partecipare a riunioni ogni qualvolta si introduca all'interno dell'ente una nuova tecnologia o debbano essere attuate compagne o operazioni che riguardino il trattamento dei dati personali e impostare unitamente al Titolare del trattamento la valutazione preventiva di impatto del rischio;
- partecipare a riunioni ogni qualvolta si introducano nuove misure sulla sicurezza o potenziali sistemi di controllo a distanza dei dipendenti o qualora si vogliano applicare politiche dell'ente che impattano sulla riservatezza dei dipendenti;
- fungere da punto di contatto per gli interessati in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti;
- redazione di risposte ad hoc in caso di esercizio da parte dell'interessato dei diritti previsti a suo favore e conseguente comunicazione agli altri eventuali titolari del trattamento.

La funzione può avvalersi del supporto di consulenze interne/esterne, concordate col Titolare del trattamento nell'ambito del budget assegnato. La funzione deve operare in accordo a quanto previsto nella lettera di nomina.

La funzione è membro del Team crisi come previsto dalla procedura Gestione Data Breach.

3.3 Persone autorizzate al trattamento

Le persone autorizzate al trattamento sono, in particolare, tutti coloro delle seguenti Aree :

- ✓ Area Amministrazione Generale e Finanziaria che coordina la Segreteria e il Protocollo;
- ✓ Area Servizi Ambientali;
- ✓ Area Tecnica impianti, bonifica e post-conduzioni;
- ✓ Area Partecipate, Contenzioso Tributario e Personale ;
- ✓ Ufficio addetto stampa;

Gli autorizzati del trattamento sono riportati nel registro dei trattamenti in relazione ad ogni specifica finalità.

Per l'individuazione delle persone che ricoprono le funzioni indicate o che operano presso gli uffici/aree indicate fare rifermento all'organigramma di **COVAR 14** versione in vigore disponibile all'interno della cartella privacy.

Per persona autorizzata al trattamento si intende chiunque agisca sotto l'Autorità del Titolare.

Le persone autorizzate al trattamento sono designate, singolarmente, dal Titolare del trattamento al fine di eseguire il trattamento dei dati e gestire le relative banche dati, in base alle istruzioni ricevute nonché alla mansione assegnatale. Le responsabilità sono dettagliate per iscritto nella lettera di nomina.

Le nomine delle persone autorizzate vengono verificate almeno annualmente ed aggiornate in occasione di introduzione di nuovi collaboratori, cambio mansioni, dimissioni, ecc.

Le nomine sono conservate presso la Segreteria/Area Ammin. e Finanziaria e nella cartella Privacy.

3.4 Data manager *e* Privacy Officer

Tra gli autorizzati sono stati designati il cd Data Manager ed i cd Privacy Officer dal Titolare del trattamento. Tali figure pur non essendo espressamente previste dal Regolamento Eu 16 /679, le si considera come una misura di mitigazione del rischio

avendo in capo le responsabilità specificate nella delibera del CdA n. 9 del 06 03 2019, nella lettera di nomina conservata agli atti.

Il Data manager è colui che coordina i Privacy Officer ed è il primario punto di contatto del DPO.

I principali compiti del Privacy Officer comprendono:

- Monitoraggio delle disposizioni legislative in materia di protezione dei dati e comunicazione al personale
- Collaborazione con il Titolare del trattamento, le persone autorizzate del trattamento, l'amministratore di sistema e soggetti esterni, finalizzata all' attuazione delle prescrizioni del Garante per la Privacy, del Gruppo 29;
- Individuazione, assieme al Titolare del trattamento, degli opportuni interventi applicativi delle norme in materia di protezione dei dati, anche a seguito di modifiche legislative;
- Collaborazione con il Titolare del trattamento per la programmazione e realizzazione di interventi formativi e di aggiornamento del personale in materia di protezione dei dati e sulle misure di sicurezza adottate (autonomamente o con la consulenza di esperti esterni)
- Assistenza agli autorizzati nell'applicazione della normativa, anche a seguito di modifiche legislative.

Alcune di queste funzioni sono membri del Team crisi come previsto dalla procedura Data Breach.

Le nomine sono conservate presso Segreteria/Area Ammin. e Finanziaria.

COVAR 14 ha nominato i seguenti Data Manager e Privacy Officer :

Data Manager Area e privacy Officer Amministrazione Generale e Finanziaria: Marina Toso

Privacy Officer Area Servizi Ambientali: Toniolo Najda

Privacy Officer Area Tecnica Impianti: Tonin Silvia

Privacy Officer Area Partecipate, Contenzioso Tributario e Gestione Personale: Fedele Nadia

.*3.5* Privacy officer It - Amministratore di sistema

Tra i Privacy Officer v'è la funzione di amministratore di sistema che è delegata, dal Titolare del trattamento, ad accedere al server di rete tramite la password di sistema e accedere ai dati di un utente assente, in caso di oggettive necessità di lavoro e sicurezza.

L'Amministratore di Sistema supporta il Titolare del trattamento dei dati personali nella valutazione dell'attuale sistema informatico in una prospettiva di sviluppo, contribuendo alla scelta di soluzioni (acquisti o modifiche al sistema) che, valutando da una parte le esigenze fondate del personale e dall'altra le possibilità tecniche di hardware e software offerte dal mercato, diano priorità al rapporto costi e profitti e possano al contempo assicurare l'impiego efficiente dell'informatica all'interno di **COVAR 14.**

I principali compiti del ADS nei confronti di **COVAR 14**, in relazione agli aspetti relativi all'applicazione del Regolamento Privacy sono:

- Garanzia di un funzionamento del sistema informatico sicuro e affidabile, attraverso il regolare monitoraggio dello stato dell'hardware e del software,
- Assicurazione della manutenzione del sistema;
- Assistenza al personale in caso di guasti o errori del sistema o modifiche al sistema stesso;
- Aggiornamento dell'antivirus;
- Esecuzione e controllo giornaliero del back up;
- Ripristino dell'intero sistema o di singoli file in caso di necessità, anche con il supporto del fornitore esterno;
- coadiuvare il Titolare del trattamento dei dati nel valutare e predisporre gli interventi da effettuare in ottemperanza alla normativa in materia di protezione dei dati.
- supporto agli utenti a livello informatico e interfaccia tra le risorse interne e il fornitore esterno di servizi assistenza informatica HW e SW.

La funzione fa riferimento al Titolare del trattamento ed è membro del Team crisi come previsto dalla procedura Gestione Data Breach.

Per quanto concerne la funzione da Privacy Officer It - Amministratore di sistema, tale ruolo è ricoperto da una Società esterna Pegaso 03 srl che per tale ragione è stata nominata responsabile del trattamento. Tale Società ha individuato nel Dott. Stefano

Occelli colui che si occuperà della parte It di Covar 14. Il contratto a responsabile del trattamento è conservato La nomina è conservata presso l'ufficio amministrazione e nella cartella privacy.

4. RESPONSABILI ESTERNI

Il responsabile del trattamento è definito dall'art. 4. 8 del Regolamento europeo come la "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".

E' il Titolare del Trattamento che nomina il responsabile scelto tra soggetti in grado di garantire il pieno rispetto del regolamento europeo privacy, la completa tutela dei diritti dell'interessato e l'adozione di misure tecniche e organizzative idonee a proteggere i dati personali affidatigli. Può essere scelto sia all'interno della struttura sia all'esterno.

Il Regolamento Privacy Europeo impone al Titolare del trattamento e al Responsabile trattamento dati di stipulare, prima dell'inizio delle attività di trattamento, uno specifico contratto di nomina che disciplini i seguenti ambiti:

- oggetto e durata del trattamento
- doveri e compiti del responsabile del trattamento
- ambito e rischi del trattamento
- natura e finalità del trattamento
- modalità di svolgimento delle attività di trattamento
- tipo di dati personali trattati
- categorie di persone fisiche coinvolte
- obblighi e i diritti del titolare del trattamento

Il contratto di nomina del responsabile del trattamento deve essere:

- redatto per iscritto
- in formato cartaceo o in alternativa in formato elettronico
- sottoscritto da entrambe le parti
- realizzato sulla base di una normativa europea o di un'altra legge di uno degli Stati Membri.

Il Regolamento specifica che il responsabile del trattamento dati non può svolgere alcun trattamento per conto del Titolare senza aver prima ricevuto precise istruzioni in merito.

Nel caso in cui un responsabile non rispetti le clausole previste dal contratto di nomina o non si attenga alle istruzioni impartite per il trattamento e con il suo comportamento determini in maniera autonoma le finalità e gli strumenti utilizzati per il trattamento, assumerà di fatto il ruolo di Titolare di trattamento.

Tale inadempimento determinerà, pertanto, una situazione di contitolarità, con la conseguenza che entrambi i soggetti saranno chiamati a rispondere in solido per gli eventuali danni cagionati agli interessati i cui dati sono stati oggetto delle attività di trattamento.

Nel caso in cui le attività di trattamento delegate al Responsabile del trattamento siano particolarmente complesse o onerose, l'art. 28.4 prevede **la designazione di un secondo Responsabile**. Tale designazione deve avere lo stesso contenuto del contratto previsto per il primo responsabile.

Il Responsabile ha, quindi, facoltà di nominare un altro Responsabile previa autorizzazione scritta da parte del Titolare

In caso di violazioni degli obblighi in capo al secondo Responsabile ne risponderà il primo, quindi, in capo ad esso sussisterà sia una culpa in eligendo sia una culpa in vigilando.

Con il suddetto contratto le società nominate Responsabili del trattamento sono formalmente impegnate ad operare nel rispetto della normativa vigente e a garantire la segretezza delle informazioni riservate a cui dovessero accedere nell'esecuzione del proprio lavoro, nonché ad attestare per iscritto la conformità degli interventi effettuati sul sistema. L'elenco dei responsabili esterni viene aggiornato annualmente.

I Responsabili esterni possono essere chiamati a far parte del Team come previsto dalla procedura Gestione Data Breach.

4.1 In **COVAR 14,** i Responsabili esterni del Trattamento sono indicati nel registro della proivacy .
I contratti in originale dei Responsabili esterni del trattamento in vigore, sono conservati presso la Segreteria/Area Ammin. e Finanziaria.

4.2 COVAR 14 nomina Subresponsabili del trattamento

L'unica nomina di COVAR 14 come subresponsabili del trattamento risulta essere quello effettuato alla società Pegaso 03 srl con contratto di nomina salvato sul programma della privacy nella categoria responsabili esterni in quanto il programma non prevede quella fattispecie giuridica. Il contratto è conservato agli atti presso la Segreteria/Area Ammin. e Finanziaria

4.2 COVAR 14 in qualità Responsabile Esterno

COVAR 14 ha inviato a tutti i Comuni il contratto di nomina di responsabile esterno per il trattamento dei dati relativi ai servizi prestati in delega delle funzioni di gestione del sistema integrato dei rifiuti e della Tari, al fine di conseguire una uniformità di impostazione complessiva.

COVAR 14 ha sottoscritto le nomine come responsabile esterno del trattamento dei dati del Titolare registrate a sistema .

5. PROFESSIONISTI ESTERNI CHE TRATTANO DATI PER CONTO DI COVAR 14

COVAR 14 in caso di incarichi a professionisti esterni, in virtù della tipologia dei dati trattati e dei rischi a cui possono incorrere, si prevede un'informativa con prescrizioni in merito al trattamento dei dati, le comunicazioni sono agli atti e conservate presso la Segreteria/Area Ammin. e Finanziaria

COVAR 14 dispone di un sito internet, che ad oggi può raccogliere dati personali per le seguenti finalità:

- per rispondere a domande/ suggerimenti;
- per invio di informazioni riguardanti l'attività svolta da Covar 14

Alla luce di quanto sopra è stata predisposta la policy privacy, la cookie policy e l'informativa news lettera conservate agli atti e debitamente pubblicate sul sito istituzionale.

7. DIRITTI DEGLI INTERESSATI

L'interessato del trattamento è la persona fisica a cui si riferiscono i dati personali.

È opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche.

I diritti esercitabili dall'interessato sono i seguenti:

- Informativa (affrontata nel paragrafo 4);
- Accesso;
- Oblio;
- Integrazione, rettifica;
- Opposizione;
- Reclamo;
- Portabilità;
- Limitazione del trattamento.

Il titolare del trattamento, a seguito di esercizio dei diritti di cui all'elenco precedente fornisce le informazioni richieste "senza ingiustificato ritardo" ai sensi dell'art 12 del Regolamento e comunque entro un mese, prorogabili di altri 2, in casi di particolare complessità.

In ogni caso il Titolare deve entro un mese informare l'interessato di tale proroga e dei motivi alla base di essa o ancora del motivo dell'inottemperanza informando l'interessato anche della possibilità di proporre reclamo o ricorso all'autorità giudiziaria.

Qualora il trattamento consista in una notevole quantità di informazioni all'interessato può essere richiesto di precisare le informazioni o le attività di trattamento a cui la richiesta si riferisce.

Le informazioni richieste dall'interessato sono gratuite.

In caso di richieste manifestamente infondate o eccessive o qualora siano richieste più copie spetta al titolare stabilire l'ammontare da chiedere facendo riferimento ai costi amministrativi sostenuti.

Il riscontro all'interessato di regola deve avvenire in **forma scritta** anche attraverso strumenti elettronici che ne favoriscano l'accessibilità. Esso può essere fornito oralmente purchè sia comprovata con altri mezzi l'identità dell'interessato.

Gli interessati potranno scrivere agli indirizzi mail indicati specificatamente nell' informativa e predisposti ad hoc per **COVAR 14** ossia: infoedatabreach@covar14.it

7.1 Diritto di accesso ex art. 15 GDPR

L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, se è in corso tale trattamento, l'accesso ai dati e alle seguenti informazioni:

a. finalità del trattamento;
b. categorie di dati personali in questione;
c. destinatari o le categorie di destinatari a cui i dati personali sono o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali (compreso il diritto di essere informato circa l'esistenza di garanzie adeguate relative al trasferimento);
d. quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare questo periodo (diritto dal quale discende l'obbligo per i titolari del trattamento di dotarsi di adeguate data retention policy o di un "Manuale della Conservazione" utile anche ai fini privacy);
e. l'esistenza del diritto dell'interessato di chiedere la rettifica, la cancellazione o la limitazione del trattamento dei dati personali che lo riguardano o del loro trattamento;
f. il diritto di proporre reclamo a un'Autorità di controllo;
g. qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h. l'esistenza di un processo decisionale automatizzato, compresa l'eventuale attività di profilazione (come da nuova definizione) nei confronti dell'interessato al trattamento.
i. In ultimo, qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

7.2. Diritto di rettifica ex art. 16 GDPR

L'interessato ha diritto di ottenere dal titolare la rettifica di dati inesatti o l'integrazione di informazioni incomplete.

La rettifica può riguardare soltanto dati oggettivi e non anche dati valutativi.

7.3. Diritto all'oblio ex art. 17 GDPR

Il diritto all'oblio consiste, quindi, nel diritto di un individuo ad essere dimenticato o non più ricordato per fatti che lo riguardano, per esempio, per condanne.

L'individuo ha diritto ad ottenere dal titolare del trattamento la cancellazione dei dati personali senza ingiustificato ritardo qualora:

- i dati non siano necessari rispetto alle finalità;
- revochi il consenso;
- si opponga al trattamento;
- sia in presenza di un trattamento illecito;
- si provveda alla cancellazione per adempiere ad un obbligo legale;
- i dati siano stati raccolti relativamente all'offerta di servizi della società dell'informazione.

Il titolare del trattamento a seguito della richiesta adotta le misure ragionevoli per informare i titolari del trattamento che stanno trattando i dati della richiesta.

Quanto sopra non si applica nei casi in cui il trattamento sia necessario:

- Per l'esercizio del diritto di libertà di espressione;
- Per l'adempimento di un obbligo legale dell'UE o dello stato membro;
- Per motivi di interesse sanitario ex art. 9;
- Ai fini di archiviazione per pubblico interesse ex ricerca scientifica o storica;
- Per l'accertamento esercizio o la difesa di un diritto in sede giudiziaria.

La cancellazione deve essere definitiva e riguardare ogni copia o riproduzione.

Nel caso in cui i dati siano stati diffusi dal titolare del trattamento è necessario notiziare i terzi.

Vi sono due possibilità:

- il caso in cui siano stati resi pubblici pertanto diffusi verso una serie di soggetti indeterminati;
- siano stati comunicati ad una serie di soggetti precisi e quindi contattabili dal soggetto titolare.

Nel primo caso il titolare dovrà farsi carico nei limiti di un canone di ragionevolezza, che tenga conto di costi e tecnologie disponibili, di informare gli altri titolari che abbiano raccolto i dati di cui l'interessato ne richiede la cancellazione da qualsiasi link, si pensi, ad esempio, alle pagine Google, ossia, i motori di ricerca che mettono tipicamente a disposizione degli utenti una copia cache delle pagine indicizzate.

Nel secondo caso, è necessario comunicare a ciascuno dei destinatari l'avvenuta cancellazione con il limite dello sforzo sproporzionato e di conseguenza i destinatari dovranno a loro volta cancellare i dati.

7.4. Diritto alla limitazione del trattamento ex art. 18 GDPR

Il Diritto alla limitazione del trattamento che è una novità assoluta rispetto il codice Privacy.
Tale norma specifica i casi in cui l'interessato può esercitare tale diritto ossia:

- Qualora l'interessato contesti l'esattezza dei dati per il periodo necessario alla verifica di tali dati;
- Il trattamento sia illecito e l'interessato si opponga alla cancellazione e chieda che ne sia limitato l'uso;
- Qualora al titolare non servano più, ma siano necessari all'interessato per finalità giudiziarie.

Sono, quindi, tutti casi peculiari, nei quali i dati devono essere trattati solo ai fini della loro conservazione, salvo che vi sia il consenso dell'interessato al trattamento per fini diversi, o esso sia necessario per l'esercizio o la difesa di un diritto in sede giudiziaria, per la tutela dei diritti di un'altra persona fisica o giuridica o per motivi di interesse.
Il Diritto è esercitato esclusivamente nei confronti del titolare, il quale a sua volta può derogare responsabili e personale dipendente.
Il titolare deve portare la richiesta di limitazione del trattamento a conoscenza di ciascuno dei soggetti a cui dati erano stati comunicati salvo che ciò sia impossibile o sproporzionato.

La limitazione può essere, successivamente, revocata e, in tal caso, prima che la revoca abbia efficacia, il titolare del trattamento deve informarne il soggetto interessato.

Tale considerando, quindi, individua le modalità per limitare il trattamento, in particolare:

- trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento;
- rendere i dati personali selezionati inaccessibili agli utenti;
- rimuovere temporaneamente i dati pubblicati da un sito web.

Va precisato che tali modalità sono a titolo esemplificativo e non esaustivo.
Il Garante nella "Guida Pratica all'applicazione del Nuovo Regolamento raccomanda" che i dati oggetto di limitazione siano "contrassegnati".

7.5. Diritto alla portabilità ex art. 20 GDPR

Il diritto alla portabilità consiste nella possibilità di ottenere dal titolare del trattamento in formato strutturato i dati personali che lo riguardano e trasferirli ad un altro titolare del trattamento senza ulteriori adempimenti a carico del titolare che li ha ricevuti, qualora si basino sul consenso o il trattamento sia effettuato con mezzi automatizzati.
Sulla base di tale definizione, il diritto alla portabilità si applica quando l'interessato abbia fornito i dati personali sulla base:

- del consenso o di un contratto;
- il trattamento sia effettuato con mezzi automatizzati;

Il gruppo WP 29 ha statuito che per "dati portabili" devono essere intesi:

- dati forniti consapevolmente dall'interessato: indirizzo postale, nome utente, età, ecc.;
- dati forniti dall'interessato attraverso la fruizione di un servizio o l'utilizzo di un dispositivo, come ad esempio, la cronologia delle ricerche effettuate dall'interessato, dati relativi al traffico, dati relativi all'ubicazione nonché altri dati grezzi come la frequenza cardiaca registrata da dispositivi sanitari o di fitness.

Con l'espressione "forniti da", ci si riferisce "ai dati personali relativi ad attività compiute dall'interessato o derivanti dall'osservazione del comportamento di tale interessato, con esclusione dei dati derivanti dalla successiva analisi di tale comportamento"[7].

Va osservato come il diritto alla portabilità comprenda:

[7] Linee Guida sul diritto alla portabilità dei dati Wp 29 del 5.4.17

- Il diritto dell'interessato di ricevere dati personali che lo riguardano trattati da un titolare e di conservarli per un utilizzo ulteriore. In tal senso può essere considerato come "un'integrazione del diritto di accesso"[8];
- Il diritto di trasmettere dati personali da un titolare del trattamento a un altro titolare del trattamento;
- La titolarità del trattamento.

L'"ex titolare" non è responsabile dell'osservanza delle norme in materia di protezione dei dati da parte del titolare ricevente, visto che quest'ultimo non è da lui selezionato.
D'altro canto il titolare ricevente è tenuto a garantire che i dati forniti siano pertinenti e non eccedenti rispetto al nuovo trattamento svolto ed è soggetto al rispetto dei principi fissati nell'art. 5 del RGPD, pertanto, il "nuovo" titolare deve specificare con chiarezza le finalità di ogni nuovo trattamento prima che sia formulata la richiesta di trasmessione diretta dei dati portabili.

7.6. Diritto di opposizione ex art. 21 GDPR

Il diritto di opposizione consente all''interessato di opporsi "in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano". A seguito dell'esercizio di tale diritto il titolare può continuare a trattare i dati solo ove "dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria".

7.7. Processo decisionale automatizzato relativo alle persone fisiche compresa la profilazione ex art. 22GDPR

L'art 4 par 4 del Regolamento definisce cosa si intende per profilazione ossia "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica".

[8] Linee Guida sul diritto alla portabilità dei dati Wp 29 del 5.4.17

L’interessato ha diritto di non essere sottoposto ad una decisione basata solo su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano e che incida sulla sua persona”.

Va evidenziato, in primis, che è l’unica norma ad essere formulata in forma negativa.
Il diritto, quindi, a non essere sottoposto ad un trattamento automatizzato, può essere derogato qualora:

a. sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
b. sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;
c. si basi sul consenso esplicito dell'interessato.

L’interessato in ogni caso ha diritto di “di ottenere l'intervento umano da parte del titolare del trattamento di esprimere la propria opinione e di contestare la decisione”.

7.8. Informativa e Consenso

7.8.1 Informativa

Il Titolare del trattamento deve fornire all’interessato tutte le informazioni e le comunicazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

Il soggetto tenuto a fornire l’informativa è il titolare, tuttavia, egli può poi delegare il responsabile o altri incaricati.

Per informativa si intende quell’insieme di informazioni che il titolare del trattamento è tenuto a fornire ad ogni interessato, verbalmente o per iscritto.

Il contenuto delle informazioni da fornire all’interessato è leggermente differente a seconda che i dati siano raccolti presso l’interessato (art.13) o presso terzi (art. 14).

Di seguito uno schema che raffronta le ipotesi di informativa sopra indicate:

ART13	ART 14
Identità e dati di contatto del titolare, responsabile e/o rappresentante del trattamento	=
Contatti DPO	=
Finalità del trattamento e base giuridica	=
Se basato su legittimo interesse spiegarlo	=
I destinatari dei dati	=
Intenzione di trasferire i dati ad un paese Terzo o ad un'org internazionale	=
Il periodo di conservazione dei dati o se non è possibile i criteri utilizzati per determinare il periodo	=
Il diritto dell'interessati di chiedere accesso, rettifica, cancellazione o limitazione del trattamento di opporsi al trattamento	=
In caso di trattamento di dati particolari ex art 9 la possibilità di revoca del consenso salvo quanto trattato fino a quel momento	=
Diritto di proporre reclamo	=
Se la comunicazione dei dati personali è un obbligo statutario o contrattuale o requisito necessario per la conclusione del contratto e se ha l'obbligo di fornirli ed eventuali conseguenze	L a fonte da cui hanno origine i dati personali e, se del caso l'eventualità che i dati provengano da fonti accessibili al pubblico
L'esistenza di un processo decisionale automatizzato e compresa la profilazione e informazioni sulla logica utilizzata	=
	Le categorie di dati personali

La raccolta ex art 13 non ha come presupposto fondamentale un contatto tra il titolare e l'interessato, ciò che conta è che la fonte di provenienza dei dati sia immediatamente l'interessato e non un altro titolare del trattamento, di conseguenza, è possibile una raccolta a distanza.

L'informativa deve essere fornita al momento della raccolta presso di sé ma prima del trattamento o, se i dati sono ottenuti da altra fonte in un tempo ragionevole, in funzione delle circostanze del caso ma in ogni caso **entro un mese** dall'ottenimento dei dati personali o al più tardi al momento della prima comunicazione o della prima rivelazione.

Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento è necessario che il titolare fornisca all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente.

Il Regolamento, nel caso in cui i dati siano raccolti presso terzi, disciplina delle eccezioni all'obbligo di fornire l'informativa, in particolare, qualora:

- l'interessato disponga già dell'informazione;
- la registrazione o la comunicazione dei dati siano previste dalla legge;
- informare l'interessato si rilevasse impossibile o richiederebbe uno sforzo sproporzionato.

COVAR 14, ha predisposto le seguenti informative interne (Allegati) al fine di adempiere a quanto richiesto dal Regolamento europeo:

- informativa visitatori;
- informativa stagisti;
- informativa selezione del personale;
- informativa dipendenti;
- informativa consulenti;
- informativa utenti;
- informativa fornitori;
- Informativa numero verde

7.8.2 Consenso

Il Consenso è definito come "qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento".

Il consenso:

- non deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è una modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" e specifico in particolare per i dati sensibili;

- deve essere in grado di dimostrare che l'interessato lo ha prestato per uno specifico trattamento;
- deve essere manifestata attraverso una "dichiarazione o azione positiva inequivocabile";
- può essere revocato dall'interessato in qualsiasi momento. Tale revoca non pregiudica la liceità del trattamento basata sul consenso conferito in un momento antecedente la revoca stessa.

Al fine di ricevere un consenso specifico è necessario verificare che la richiesta sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio all'interno di modulistica.

In merito al trattamento di dati particolari (dati sanitari) il trattamento avviene con il consenso esplicito e specifico dell'interessato.

8. Analisi dei rischi

Premessa

L'art 32 del Regolamento prevede le c.d misure di sicurezza a mente del quale il titolare ed il responsabile del trattamento devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Con il termine rischi del trattamento si fa riferimento a:

- rischi materiali come la distruzione accidentale o illegale dei dati, la perdita, la modifica, la rivelazione di dati o l'accesso non autorizzato a dati o –
- rischi immateriali come la perdita di controllo sui dati personali, la limitazione dei diritti dell'interessato, la discriminazione, il pregiudizio alla reputazione, la perdita di riservatezza.

Gli adempimenti, quindi, richiesti al titolare del trattamento sono:

1) **valutazione dei rischi** aventi ad oggetto il trattamento, dovranno, pertanto, essere presi in considerazione i fattori di rischio sopra elencati. In caso di rischio elevato sarà necessario, come si vedrà meglio in seguito, una valutazione d'impatto ed eventualmente anche la consultazione preventiva al Garante.
2) **messa in atto di misure per limitare i rischi** tenendo in considerazione lo stato dell'arte, i costi di attuazione, natura, oggetto contesto e finalità del trattamento i rischi per i diritti e le libertà delle persone fisiche. Le misure possono essere:
   - **TECNICHE** che si concretizzano in:

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

Detta lista di cui al paragrafo 1 dell'art. 32 è una lista esemplificativa e non esaustiva.

- **ORGANIZZATIVE** che si concretizzano:
  a. nelle designazioni che prevedono una distribuzione delle responsabilità tra titolare e responsabili;
  b. nell'adozione da parte del titolare del trattamento o dal responsabile di politiche adeguate;
  c. nell'adesione a codici di condotta o certificazioni.

COVAR 14 e ciascun Responsabile del trattamento mettono in atto a fronte dei pericoli individuati misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

8.1 Fonti di pericolo

Buona parte dei danni può insorgere da parte sia di collaboratori dell'azienda sia di terzi:

- involontariamente (errori di manipolazione);
- per negligenza (inavvertenza, leggerezza);
- in mala fede (atto criminale).

I rischi possono essere causati da:

- Comportamenti degli operatori
  Furto di credenziali di autenticazione

Carenza di consapevolezza, disattenzione o incuria

Comportamenti sleali o fraudolenti

Errore materiale

- Eventi relativi agli strumenti

  Azione di virus informatici o di codici malefici

  Spam o altre tecniche di sabotaggio

  Malfunzionamento, indisponibilità o degrado degli strumenti

  Accessi esterni non autorizzati

  Intercettazione di informazioni in rete

- Eventi relativi al contesto

  Accessi non autorizzati a locali/reparti ad accesso ristretto

  Asportazione e furto di strumenti contenenti dati

  Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria

  Guasto ai sistemi complementari (impianto elettrico, climatizzazione)

  Errori umani nella gestione della sicurezza fisica.

8.1.2 Misure tecniche ed organizzative

Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Costituiscono misure tecniche ed organizzative che possono essere adottate dal Servizio cui è preposto ciascun Responsabile del trattamento:

- sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);
- misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione

di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.

COVAR 14 e ciascun Responsabile del trattamento si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

I dati di contatto del Covar 14sono pubblicati sul sito istituzionale.

L'adozione di adeguate misure di sicurezza è lo strumento fondamentale per garantire la tutela dei diritti e delle libertà delle persone fisiche. Il livello di sicurezza è valutato tenuto conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali COVAR 14 essi, conservati o comunque trattati. L'efficace protezione dei dati personali è perseguita sia al momento di determinare i mezzi del trattamento (fase progettuale) sia all'atto del trattamento.

8.2 Premessa IT

Nel Regolamento Europeo 2016/679 l'analisi del rischio privacy ha un ruolo fondamentale: diventa lo strumento atto a dimostrare l'adeguatezza delle misure implementate a tutela dei dati trattati per dimostrare l'"accountability" dell'Azienda rispetto al GDPR. L'"*Analisi dei rischi*" di partenza effettuata nel Settembre 2018 è allegata alla delibera di cda n. 9 del 06 03 2019. La gestione e le misure tecniche sono affidate a Pegaso03 S.r.l. vengono quindi riportate per correttezza tutte le misure tecnico organizzative adottate da Pegaso03 S.r.l. a tal proposito.

8.2.1 Analisi dei Rischi

Nel Regolamento Europeo 2016/679 l'analisi del rischio privacy ha un ruolo fondamentale: diventa lo strumento atto a dimostrare l'adeguatezza delle misure implementate a tutela dei dati trattati per dimostrare l'"accountability" dell'Azienda rispetto al GDPR. allegato alla delibera del cda n. 9 del 06 03 2019.

La struttura ad un'attenta analisi risulta essere conforme al Regolamento Europeo 679/2016. Per le valutazioni d'impatto si rimanda al documento specifico e alle procedure del Programma della Privacy.

8.2.2 Analisi della struttura

La struttura principale è sita in Via Cagliero, 3, 10041 (Carignano TO)

Nella struttura principale sono state adottate le seguenti misure di sicurezza fisiche per l'accesso ai locali:

- antifurto
- vigilanza notturna

La sala CED principale è stata ricavata all'interno di un ex vano ascensore. La porta di accesso è blindata e chiusa a chiave. Le chiavi sono a disposizione del solo reparto IT e il responsabile delle chiavi è il responsabile IT. All'interno di tale locale è presente un climatizzatore per garantire una temperatura e umidità costante. E' presente anche un secondo climatizzatore di backup che si attiva nel caso in cui il primo abbia un difetto e/o anomalie del primo.

All'esterno della sala CED è presente un estintore sottoposto a regolati controlli caricato con Co2. Non esiste un sensore che si attiva in caso di perdita d'acqua in quanto nel locale non vi è passaggio di tubature e non si sono verificati eventi di questo tipo negli ultimi 10 anni.

Si possono quindi riassumere le seguenti misure di sicurezza:

- locale chiuso adibito esclusivamente alla funzionalità di sala CED
- armadi rack chiusi a chiave. Le chiavi sono custodite da un responsabile IT interno alla struttura
- climatizzatore per mantenere sempre costante la temperatura all'interno della sala CED
- secondo climatizzatore nel caso in cui il primo si danneggi
- estintore Co2 in caso di incendi presente fuori la sala CED

- gruppo di continuità per proteggere la sala CED da eventuali sbalzi sulla corrente elettrica e in caso di blackout
- l'accesso alla sala CED è protetto da una porta blindata il cui accesso è limitato solo al personale IT chiuso con chiave
- pavimento flottante che protegge il rack e le componenti contenute in esso in caso di perdite d'acqua all'interno della sala CED rialzato di circa 60 centimetri

8.2.3 Asset Aziendali

La rete informatica di Covar14 è composta da n. 5 (dotazione in fase di verifica per sostituzioni) server fisici posizionati all'interno della sala CED. Inoltre sono presenti n. 31 postazioni client, n. 10 Notebook e n. 5 tablet e n. 11 smartphone dell'Ente.
La configurazione di tablet e smartphone aziendali, prima della consegna agli interessati, viene effettuata direttamente da personale del reparto IT che si preoccuperà di mettere in sicurezza, eventualmente cifrando e verificando che le misure di sicurezza siano adeguate, i dispositivi in questione.
Il BYOD (Bring Your Own Device), termine tecnico che indica la possibilità di utilizzare dispositivi personali nel posto di lavoro ed utilizzarli per accedere a informazioni aziendali e/o database, non è consentito sia per policy aziendali, come specificato nel regolamento aziendale consegnato e messo a disposizione di ogni dipendente, sia per aumentare la sicurezza IT aziendale.
Il firewall CHECKPOINT (FIREWALL UTM-1 NGX R) è in comodato d'uso con contratto di aggiornamento firmware almeno semestrale per la protezione perimetrale su tutta la rete.
La connettività è appena stata migrata a FTTC con fornitore BT con una connettività di backup attualmente tramite fornitore Vodafone.
Sono configurate una DMZ e la LAN di Pegaso03 S.r.l.

Le caselle di Posta Elettronica dei dipendenti Pegaso03 e delle varie aree, risiedono su un server IBM Verse. Il sistema IBM Verse in Cloud garantisce la distribuzione delle caselle di posta elettronica su più server ed è pertanto garantita l'accessibilità delle caselle. Inoltre è integrato un servizio antispam e antivirus incorporato nello stesso.

Eventuali documenti cancellati rimangono accessibili dal Cestino entro 90gg. poi vengono definitivamente cancellati.

Sulle caselle dei Responsabili di Area è stato attivato a inizio anno 2017 un sistema di Archive, che consente di accedere anche oltre i 90 gg. a dati storici della propria casella di Posta Elettronica.

Per le caselle di Area e caselle particolari non migrate a IBM Verse è presente la casella sul server Dompega con replica sul server Dompeg2 ogni 15 minuti.

- d:\lotus\domino\data\mail*.nsf

La gestione e le procedure riguardanti la gestione della posta elettronica sono comunque presenti nell'allegato "Sistemi informativi - PO01 - Procedure di Backup e Ripristino - v03"

Il server Proxy è SQUID su Virtual Server Ubuntu Linux nell'"Allegato server proxy" .

L'antivirus utilizzato sui client e sui server Microsoft è affidata a Symantech end point tale software integra nativamente il controllo antiransomware assicurando quindi una protezione da malware come ad esempio Cryptlocker , Wanna cry, etc

E' installata sul server la console di gestione di tale antivirus che monitora gli aggiornamenti dello stesso sia sui client sia sui server.

Tutti i client e relative utenze sono sotto server di dominio. Il sistema operativo che si preoccupa di gestire il dominio è affidato a Windows Server 2012.

L'aggiornamento degli update di Microsoft, quindi dei sistemi operativi e relativi software della stessa casa madre, viene gestito tramite policy centralizzato dal server di dominio.

Tutti gli utenti dei client hanno privilegi al massimo di net user, non è possibile quindi da parte di un utente installare programmi e/o periferiche se non tramite l'intervento del Responsabile IT.

L'inventario degli asset serve a conoscere e controllare gli elementi di un sistema di gestione per la sicurezza delle informazioni. Tra questi elementi ci sono i server, i pc, i dispositivi di uso personale, i dispositivi di rete, le sedi, gli impianti di sicurezza, gli archivi fisici, le informazioni stesse e il personale. Altri, come i redattori della ISO/IEC 27005, introducono anche i processi.

Tale documento viene aggiornato in caso di modifiche di asset effettuate all'interno del sistema informativo della Covar14e utilizzato nella policy dei dispositi "end of life".

8.2.4 Elenco dei database

Sono stati individuati, analizzando la struttura con i responsabili IT della Società, i database riportati nella seguente tabella.

Nome database/Programma	Descrizione database (tipi dati contenuti, etc)	Server Interno/Esterno	Note
FileSystem	Cartelle di rete condivise con accesso multilivello	Server Interno	
TIVOLI STORAGE MANAGER	Sistema di backup su disco fisso e su nastro	Server Interno	Fornitore IBM Tivoli
SIPAL PROTOCOLLO	E' il software per la protocollazione della posta in entrata ed in uscita	Server Interno	Fornitore SIPAL - Gruppo Maggioli
GESTIONE ANAGRAFE COMUNI	E' il software per la gestione dei dati anagrafici provenienti dai Comuni. Realizzato in casa su piattaforma DOMINO dotata di sistemi di sicurezza	Server Interno	sviluppo interno su piattaforma IBM Lotus Domino - IBM DB2
PROTOCOLLO	Casella di posta elettronica	Server Interno	IBM Lotus Domino
PEGASO CUSTOMER CARE	Software per la gestione delle chiamate utenti. Realizzato su piattaforma DOMINO che è dotata di sistemi di sicurezza.	Server Interno	sviluppo interno su piattaforma IBM Lotus Domino - IBM DB2
ARCA PROFESSIONAL	Gestionale di contabilità	Server Interno	Fornitore Artel

G.I.TAR.	E' il software per la gestione della tariffa. Realizzato in casa su piattaforma DOMINO dotata di sistemi di sicurezza.	Server Interno	sviluppo interno su piattaforma IBM Lotus Domino - IBM DB2
MODULISTICA ISO	Sviluppo interno su piattaforma IBM Lotus Domino - IBM DB2	Server Interno	Database contenitore della procedure ISO
GE.RI.	E' il trattamento dei dati utili per il recupero del credito. La banca dati è principalmente condivisa con la GESTIONE TARIFFA RIFIUTI	Server Interno	Fornitore Municipia - Engineering

La gestione di accesso ai database avviene tramite un accesso multilivello definito da un nome utente ed una password sia nel caso di accesso a cartelle condivise sia nel caso si tratti di accesso a database tramite l'utilizzo di piattaforme e/o programmi gestionali. La connessione ai server contenti i database è sicura in quanto presente all'interno della LAN.

8.2.5 Utenze ed accessi ai database

L'accesso ai database del punto precedente è regolamentato attraverso un accesso multilivello gestita a livello di gruppi di lavoro del dominio e utenze.
I gruppi e gli utenti di dominio sono gestiti dagli operatori dell'Area Sistemi Informativi ai quali viene fatta richiesta di abilitazione di nuovi utenti o autorizzazione ad accedere a cartelle di rete

Sono state disabilitate le funzionalità USB di massa ad esclusione di personale che per attività lavorative sono obbligati ad utilizzare periferiche di archiviazione di massa responsabili di funzione: qualità, IT, amministrazione, tecnico.

In alcuni uffici non si possono precludere le funzionalità USB ad esempio per apporre firma digitale tramite apposita pendrive per firmare i documenti.
Per la creazione di una nuova utenza verrà inviata dal responsabile IT una mail indicante il nome, cognome e mansione della nuova risorsa al responsabile IT che provvederà a creare l'utenza di dominio e relativa casella mail. Tale nuova utenza sarà quindi inserita nel gruppo di dominio, a seconda della mansione affidata, erediterà tutti i privilegi ai relativi accessi ai database e risorse. Il responsabile IT una volta effettuate queste operazioni provvederà ad informare il responsabile HR tramite mail dell'avvenuta creazione.
Nel caso in cui ci sia un allontanamento o licenziamento di una persona il responsabile di Area invierà una mail al responsabile IT che metterà in atto la procedura come da regolamento aziendale. Al termine di tale procedura il responsabile IT provvederà ad inviare una mail di avvenuta disattivazione dell'account affidato alla risorsa non più presente nell'Ente.

8.2.6 Misure logiche di sicurezza

Tutti i server contenti dati personali, presenti solo all'interno della sala CED.
Nella sala CED sono presenti hard disk per la sostituzione a caldo e immediata in caso di guasti.
I server presenti nella sala CED presentano le seguenti caratteristiche:

- accesso multilivello alle cartelle condivise con permessi individuati dall'utenza del dominio
- alert dei firewall abilitati che avvisano in caso di anomalie inviano mail al reparto IT
- antiransomware su server di dominio
- antivirus su server di dominio
- firewall fisico costantemente aggiornato
- impossibilità di utilizzare dispositivi personali ma solo aziendali (BYOD vietato)
- poteri al massimo di net user agli utenti di dominio quindi senza privilegi amministrativi sul pc locale
- server DHCP protetto da gruppo di continuità in caso di sbalzi di corrente e/o blackuot
- server dominio protetto da gruppo di continuità in caso di sbalzi di corrente e/o blackout

- utilizzo di group policy per decidere quali programmi possono essere eseguiti dagli utenti di dominio
- procedura per verificare l'aggiornamento e la sicurezza dei server linux

I personal computer definiti client presenti all'interno della struttura principale adottano ed hanno attive le seguenti misure di sicurezza per garantire una sicurezza adeguata come richiesto dal Regolamento Europeo 679/2016.

I pc client che si collegano ai server adottano le seguenti misure di sicurezza:

- antivirus che protegge i client in tempo reale
- antiransonware che protegge i pc in tempo reale
- aggiornamenti abilitati dell'antivirus per le ultime definizioni dei virus
- pc sono protetti da password di dominio
- le password sono composte da 8 caratteri come descritto successivamente in questo documento
- scadenza password impostata a 90 giorni per aumentare la sicurezza
- aggiornamenti del sistema operativo gestiti manualmente dal reparto IT
- screen saver impostati a 10 minuti con sblocco tramite password
- blocco delle uscite usb in modo tale da impedire uscite di dati ed impedire ad eventuali virus di propagarsi all'interno della rete LAN tramite di esse
- privilegi di net user sui pc dedicati agli utenti di dominio dove possibile
- aggiornamenti automatici abilitati per il browser predefinito
- verifiche periodiche alla ricerca di software non autorizzato installato sui client
- implementato tramite regolamento aziendale il blocco dei pc tramite la combinazione CTRL+ALT+CANC e blocca oppure tramite il tasto Windows della tastiera e L

Si tiene a precisare che al rinnovo della struttura IT tutti i dischi rigidi dei pc verranno cifrati utilizzando la funzionalità Bitlocker presente nei sistemi operativi Microsoft Professional.

Tutti i pc client presenti in Azienda ed anche per utilizzo esterno, quindi anche quelli presenti nella sede dislocata, sono protetti da nome utente e password all'accensione. La password viene cambiata ogni 90 giorni rispettando i parametri standard elencati sotto:

a) almeno 8 caratteri di cui almeno 4 delle seguenti tipologie :
    a) un carattere maiuscolo (da A a Z)

b) un carattere minuscolo (da a a z)
c) una cifra numerica (da 0 a 9)
d) un carattere non alfanumerico, come ad esempio: !,$,#.

Ogni dipendente ha una sua utenza univoca con relativa password, conosciuta solo dallo stesso, non esistono quindi profili o utenze condivise da più persone.
I database interni, considerando anche cartelle condivise contenenti dati di persone fisiche, adottano i seguenti accorgimenti:

- accesso multilivello alle cartelle condivise/database
- accesso tramite nome utente e password personali
- scadenza password utenti
- database sottoposto a backup
- backup crittografato del/dei database
- controllo periodico manuale dell'effettiva riuscita del/dei backup
- backup dislocato fisicamente rispetto alla sede centrale
- i dispositivi contenenti i backup sono protetti da gruppo di continuità
- i backup sono conservati in luoghi sicuri
- è presente versioning dei backup
- i dispositivi di backup sono basati su sistemi RAID in modo da garantire la resilienza a livello informatico
- i backup sono accessibili esclusivamente al personale del reparto IT
- possibile esportare in un formato comune i dati riguardanti una persona fisica
- possibile eliminare record contenti dati di una persona fisica
- controllo dei file di log per evidenziare evenutali databreach e/o funzionamenti irregolari del database

L'utilizzo delle VPN è consentito solo ad alcuni utenti. La connessione avviene tramite l'inserimento di credenziali, composte da nome utente e password, e autenticata tramite la gestione di certificati.
Tali connessioni hanno attive le seguenti misure tecniche:

- le connessioni VPN sono cifrate
- è presente una protezione a due fattori per l'accesso da remoto
- i file di log delle VPN vengono controllate periodicamente in modo tale da individuare eventuali accessi non autorizzati all'interno della LAN

- controllo semestrale delle utenze VPN non più attive e relativa cancellazione in caso di non utilizzo
- nel caso in cui un utente VPN dovesse inserire una password errata per più di tre volte la suddetta utenza verrà bloccata

Viene inserito "Allegato VPN" al cui interno sono presenti regole e policy riguardanti tali connessioni.

Sono altresì adottate ulteriori misure di sicurezza come da elenco seguente:

- cifratura dei portatili utilizzati esternamente all'Azienda al rinnovo dei noleggi triennali
- periferiche di archiviazione di massa cifrati in caso di spostamenti di dati personali al di fuori dei locali fisici dell'Azienda
- documento digitale contente tutti i dispositivi di archiviazione di massa con relativo nominativo di assegnazione e data di consegna
- verifica semestrale di utenze non più utilizzate e se possibile cancellate o altrimenti disabilitate all'interno del sistema
- procedura documentata con specifiche tecniche in caso di dismissione/riutilizzo hardware contente dati personali
- smartphone e/o tablet bloccati tramite pin all'accensione e all'utilizzo
- controllo giornaliero da parte del personale IT che verifica a livello visivo le funzionalità delle componenti IT presenti nella sala CED tenendo aggiornato un registro dei controlli
- protezione di dati personali inviati via mail resi sicure con tecniche di sicurezza ad esempio tramite impostazione password sugli allegati
- periferiche di archiviazione di massa cifrate o a livello hardware o a livello software

Verranno adottate e comunque prese in considerazione anche le seguenti tecniche per aumentare la sicurezza informatica secondo le scadenze indicate nella seguente tabella:

Criticità	Operazioni consigliate	Implemetata entro
Manca sensore fumi sala CED	Verificare se possibile implementare un sensore fumi che avvisi in caso di incendi collegabile all'impianto antifurto e/o che avvisi dei responsabili in caso di attivazione	

Pc portatili non hanno hard disk cifrati	Cifrare i dischi dei portatili o attraverso Bitlocker direttamente da Windows 10 o software preposti a tale scopo (esempio utility dei portatili Hp, etc)	
Mancanza controllo sui dispositivi mobile	Verificare se possibile implementare sui dispositivi mobile (tablet e smartphone) la possibilità di installare l'estensione dell'antivirus in modo tale da poter bloccare e cancellare i dati in essi contenuti anche da remoto	
Utilizzo di periferiche di archiviazione di massa non cifrate	Prevedere l'utilizzo di periferiche di archiviazione di massa cifrate o a livello hardware. Catalogare tutte le periferiche di massa in un elenco contenuto in un file digitale, al quale ha accesso solo il reparto IT, contenente nome della periferica, data di consegna, data di rientro, persona alla quale è stata consegnata. Tutte queste soluzioni vanno applicate alle periferiche che conterranno potenziali dati personali.	
Migliorare la formazione degli utenti riguardante la segretezza delle password personali	In fase di formazione di persone autorizzate al trattamento specificare di mantenere segreta la password inserendolo anche nel regolamento aziendale	
Verificare se la cartella scansioni viene cancellata con regolarità	Prevedere una policy per la cancellazione delle scansioni più vecchie, questa operazione verrà implementata per garantire la minimizzazione dei dati presenti.	
Manca procedura per le scansioni Scan to mail	Implementare procedura specificata all'interno del regolamento aziendale riguardante la gestione della modalità scan to mail	
Manca documentazione in caso di dismissione	Produrre documentazione in caso di dismissione hardware dove vengono indicate le tecniche di formattazione e le procedure utilizzate per	

hardware	cancellare dati presenti su periferiche di archiviazione di massa	
Controllo fisico della LAN	Verificare se possibile inserire un filtro mac address in modo tale da tenere sempre sotto controllo i pc che vengono collegati fisicamente alla LAN	
Abilitare screen saver sui client	Implementare sui client screen saver impostati a 5 minuti di inattività con relativo sblocco tramite password	
Aggiornamento l'elenco degli asset aziendali	Aggiornare il documento contenente gli asset aziendali. Tale documento dovrà contenere informazioni su ogni singolo asset .	
Presenza anche solo temporanea di dati personali sui client	Nel corso di formazione al personale verrà illustrato agli utenti di non salvare dati personali in locale ma solo su cartelle condivise sottoposte a backup. Tale procedura sarà integrata anche nelle policy aziendali.	
Non avete bloccato, ovvero interdetto fisicamente o tramite modifiche al sistema operativo o con software dedicati l'accesso a qualsiasi dispositivo di ingresso/uscita di informazioni come porte usb, cd rom e dvd per ogni computer in dotazione ai vostri dipendenti, per le postazioni che non	Verificare se possibile predisporre una policy a livello di dominio per cui gli utenti non siano in grado di utilizzare le porte USB, masterizzatori, lettori di carte (SD,etc) dei pc se non su richiesta al reparto IT dove possibile	

devono godere di questi privilegi		
Libero accesso a sistemi di archiviazione esterni (es: Dropbox, Google Drive, etc)	Verificare dove possibile limitare o bloccare l'utilizzo di servizi di archiviazione esterni e giustificare tramite documento anche in formato digitale per quali utenti è attivo giustificando tali scelte	
Controlli alla ricerca di materiale protetto da copyright	Predisporre una procedura grazie alla quale si ricercano materiali pornografici o protetti da copyright, Tali controlli dovranno essere documentati, anche in formato digitale, e dovranno contenere il nominativo della persona che effettua i controlli, la data e l'esito del controllo	
Manca documentazione in caso di consegna di tablet, smartphone o cellulari	Produrre documento dove vengono indicate le azioni e comportamenti da tenere in caso di consegna di tablet, smartphone o cellulari aziendali	
Verifica cloud su piattaforma Maggioli	Verificare richiedendo a Maggioli specifiche sul cloud da loro utilizzato	
Controllo file di log al database	Prevedere documento anche in formato digitale all'interno del quale verrà presa nota del risultato dell'analisi dei file di log al database alla ricerca di data breach	
Pseudonimizzazione database interni	Verificare, anche tramite richiesta mail ai fornitori delle piattaforme utilizzate, la possibilità di pseudonimizzare i database interni o eventuale cifratura di colonne per rendere database anonimo	
Manca documentazione sul controllo di	Produrre documento che verrà compilato annualmente sui dispositivi server end of life	

periferiche end of life		
Mancanza backup dislocato	Prevedere se possibile implementare un backup dislocato fisicamente rispetto la sede centrale	
Cifratura backup dislocato	Verificare se possibile, tramite il software utilizzato per i backup, cifrare i backup dislocati fisicamente rispetto la sede centrale.	
Procedura power up/shutdown per la sala CED	Prevedere un documento contenete la procedura di powerup/shutdown nella quale è presente la sequenza da rispettare in tali casi	
Acquisto di hard disk per garantire la sostituzione immediata in caso di anomalie e/o guasti sugli storage di rete	Prevedere l'acquisto di hard disk aggiuntivi da tenere all'interno della sala CED per rendere immediatamente disponibile la sostituzione in caso di guasto di uno storage di rete	
Verifica sulle impostazioni di sicurezza sulle connessioni VPN	Verificare se possibile implementare regole più rigide se un utente dovesse sbagliare la password di accesso per più di tre volte	
Richiedere documentazione sui contratti con aziende esterne	Recuperare contratti con aziende esterne, ad esempio contratti di SLA, e verificare la loro conformità con il GDPR	
Documentazione su server proxy	Produrre un documento che indica le funzioni del server proxy utilizzato in Azienda	
Produrre tabella contente i cookie presenti sul sito	Produrre tabella contente cookie e tempi di permanenza dei cookie da inserire nella cookie policy che sarà pubblicata sul sito	

L'utilizzo delle periferiche di archiviazione di massa è normato attraverso il regolamento aziendale fornito ad ogni dipendente. In tale documento infatti viene specificato che

non è possibile utilizzare supporti personali ma solo ed esclusivamente supporti forniti del reparto IT che provvederà alla messa in sicurezza degli stessi tramite cifratura o hardware o software. Ogni periferica di archiviazione di massa sarà inserita in apposito registro, anche in formato digitale, che conterrà la data di consegna, il destinatario della periferica. Inoltre come prassi verrà adottata la cifratura dei supporti anche in caso di spostamento di file al di fuori della sede centrale, ad esempio per invio di file a responsabili esterni di un trattamento.
Le scansioni effettuate all'interno dell'Azienda sono inviate tramite mail al destinatario aziendale o attraverso la condivisone di una cartella dedicata. E' stato implementato sempre tramite regolamento aziendale una procedura nella quale si specifica di cancellare la mail contenete la scansione una volta salvato l'allegato per minimizzare i duplicati dei file all'interno dei database. Inoltre la cartella predisposta alla raccolta delle scansioni verrà cancellata almeno ogni tre mesi sempre per minimizzare i duplicati dei file.

8.2.7 Criteri e modalità di ripristino dati

Valutando la struttura e relativi backup e i tempi di ripristino sono di giorni: 2 nel caso in cui sia necessario il ripristino totale dei server presenti nella sala CED fermo restando la disponibilità dell'hardware.
Nel caso in cui si tratti di recupero di dati parziali il tempo è stimato entro la giornata lavorativa e comunque legato alla mole di dati da trasferire in quanto può essere gestito in autonomia dai componenti del reparto IT.
Nel caso in cui si presenti un evento per il quale la sala CED debba essere riavviata e/o spenta esiste una procedura di shutdown/powerup documentata nell'allegato "Procedura di Power-up/Shutdown".
Il server di dominio è basato su Windows 2012 R2. Risulta quindi essere un prodotto Microsoft ancora supportato per gli aggiornamenti sulla sicurezza.

Il backup viene gestito da una macchina (TSMPEGA) dove è installato il software di backup e ripristino chiamato IBM Tivoli Storage Manager che fa capo ai Client installati sui server, contenenti i dati, della rete aziendale.

Il Tivoli Storage Manager detto anche TSM è un software per la gestione delle operazioni di backup e ripristino di dati che basa il suo funzionamento su due interessanti concetti: la gestione gerarchica dello storage ed il paradigma di backup chiamato *incremental forever*. Di base il software presenta un elemento centrale composto dall'engine vero e proprio e dal data base dei dati (un'istanza DB2), il tutto gestibile tramite i comandi TSM a console o, più semplice ma meno agile, tramite un'interfaccia web basata su Websphere che ha nome Integrated Solution Console (ISC). Sui server che si desidera sottoporre a backup viene invece installato un client che funge da agente oltre ad essere interfaccia di gestione di molte altre attività: TSM Backup Archive Client.

Il funzionamento base è banale: a livello server vengono definiti gli storage pool (i contenitori in cui verranno posizionati i dati sottoposti a backup), le policy (le regole a cui sottostanno i job di backup) ed i nodi (i server soggetti a backup). Una delle particolarità di TSM è la gestione gerarchica degli storage pool che consente di definire, all'interno di una policy, uno storage pool pregiato come primo contenitore dei dati salvati e, in base al riempimento, TSM si occuperà di spostare i dati in storage pool meno pregiati.

Tipicamente in TSM è quindi possibile dedicare delle aree di disco preallocato (con accesso in scrittura random) di modeste dimensioni (50-100 GB) su cui viene eseguito il backup. Al riempimento di queste aree i dati più vecchi vengono spostati in storage pool gerarchicamente successivi, solitamente composti da volumi di tipo nastro LTO, molto più capienti e molto più lenti in scrittura e lettura rispetto ai volumi di tipo disco. Il vantaggio di questa architettura sta nel fatto che i dati scritti di recente sono disponibili su volumi sempre online, cosa che agevola notevolmente il ripristino dei file se contenuti in backup recenti. L'impiego de volumi nastro per le eccedenze garantisce la disponibilità di spazio a "basso costo" per il sistema di backup.

L'altra funzionalità estremamente utile è la politica con cui vengono eseguite le schedulazioni di backup incrementale. I sistemi "classici" si limitano ad eseguire backup FULL periodici intervallati da una serie di backup INCR (incrementali), tipicamente si esegue un FULL tutte le domeniche e sei INCR dal lunedì al sabato. Considerando una profondità di backup di un mese ci troveremmo a dover conservare quatto occorrenze FULL e ventiquattro occorrenze INCR.

Il paradigma *incremental forever* è più semplice e molto più efficace. Questa tecnica prevede che venga eseguito un primo backup FULL dei dati seguito da un certo numero di backup INCR perpetui al fine di salvare, di giorno in giorno, tutti i file che subiscono modifiche. A questa politica viene assegnato un limite che corrisponde al numero di versioni di un certo file che si desidera mantenere. Riprendendo l'esempio fatto poco fa ci potremmo limitare all'esecuzione di un primo backup FULL in un giorno X e schedulare un backup INCR giornaliero definendo di mantenere le ultime ventotto versioni di ogni file salvato. In questo modo, anche se un file venisse modificato tutti i giorni, avrò la certezza di avere a disposizione le ultime ventotto versioni del file corrispondenti agli ultimi ventotto giorni di backup.

Il vantaggio di questo paradigma si legge in due considerazioni:

- Laddove un file non venisse modificato tutti i giorni si ottiene che le ventotto versioni conservate faranno riferimento anche a periodi di tempo antecedenti all'ultimo mese solare, incrementando quindi l'efficienza del sistema senza inficiare il consumo della risorsa storage.
- Lo storage pool definito per la politica di backup conterrebbe un solo backup FULL in luogo dei quattro backup FULL del primo esempio risparmiando così quantitativi notevoli di risorse storage.

Tutti gli archivi oggetto di trattamento sono contenuti su diverse macchine Server. Su queste ultime è installato il software TSM Backup Archive Client che dialoga con il TSM Server. Il client TSM è un agente che opera sulle stazioni per cui si rende necessario eseguire il salvataggio, ed è colui che inizia le operazioni relative a salvataggi e ripristini delle informazioni, dati e applicazioni. Il client TSM dialoga con l'ambiente Server utilizzando il protocollo di comunicazione standard TCP/IP.

Il software IBM Tivoli Storage Manager Backup Archive Client è installato su tre macchine differenti:

Dompeg2, che contiene tutti gli archivi di Posta Elettronica, gli Applicativi Pegaso e il cervello del sistema

Ammpeg2, che contiene il software di gestione del Protocollo con la relativa base dati (SIPAL), l'area di scambio per l'Amministrazione ed il Personale, il software delle Presenze (Lora), il software della contabilità (Arca Professional) e la copia deil Database DB2 Pegaso.

Bl-srv-01, che contiene tutta l'area di Scambio Pegaso.

Il Server TSM è collegato tramite connettore SAS a 6Gbps ad un sistema chiamato IBM System Storage TS3100 Tape Library Express che permette di poter effettuare il backup dei dati, precedentemente salvati localmente sulla macchina Tsmpega, su nastri LTO (Linear Tape-Open). La libreria a nastro TS3100 è configurata con due caricatori rimovibili di cartucce, uno a sinistra (12 slot per cartucce) e uno a destra (12 slot per cartucce). Inoltre, il caricatore di sinistra include uno slot dedicato alla posta che ha il compito di supportare i continui scambi con la libreria durante l'importazione e l'esportazione dei supporti. La libreria è dotata di lettore di codice a barre che supporta le operazioni con accesso sequenziale o causale. TS3100 include di serie funzioni di gestione remota, per consentire l'amministrazione remota della libreria di nastri tramite un'interfaccia Web. Path Failover è una funzione opzionale di questa libreria studiata per assicurare il fai lover automatico del percorso di controllo a un percorso di controllo ridondato preconfigurato, nel caso in cui un adattatore host o un percorso di controllo venga perso interrompendo il lavoro in corso.

La tecnologia IBM Ultrium 5 assicura maggiore capacità e supporto continuo per la crittografia dei dati. Il core di crittografia e decrittografia hardware ed il core di controllo risiedono nell'unità nastro IBM Ultrium 5. Un buffer dati interno più ampio nell'unità ad altezza completa contribuisce a migliorare la velocità di accesso ai dati e ridurre i tempi di riempimento e avvolgimento delle cartucce con la calibrazione dinamica del canale, per aumentare il throughput (*la quantità di dati trasmessi in una unità di tempo*) dei dati. Oltre a leggere e scrivere su cartucce nastro LTO Ultrium 5, l'unità nastro LTO 5 è in grado di leggere e scrivere su cartucce LTO 4 e leggere cartucce LTO 3 con velocità più elevate. Le unità nastro IBM Ultrium 5 sono concepite per supportare velocità di trasferimento dati di 140MBps e una capacità fisica nativa di 1,5TB su cartucce dati IBM System Storage Ultrium da 1,5TB (3,0TB con compressione 2:1). Il sistema TS3100 con unità nastro Ultrium 5 ha una capacità nativa di 36TB (72con compressione 2:1). Le unità nastro IBM LTO 4 invece supportano fino a 120MBps di velocità di trasferimento dati nativa. Inoltre il sistema TS3100 con unità nastro Ultrium 4 ha una capacità nativa fino a 19,2TB (38,4TB con compressione 2:1).

La finestra di Backup, nella quale vengono effettuate le operazioni di copia, è schedulata quotidianamente in notturna per evitare problemi di accesso multiplo sui file

e/o database da parte degli utenti che giornalmente ci lavorano. Il backup dei dati può avvalersi di una profondità di 15 versioni.
Procedure di ripristino:

Una situazione di *Disaster* può presentarsi in qualsiasi momento e può essere innescata da diversi fattori:

- Problemi Hardware
- Problemi Software
- Problemi legati all'ambiente
- Errori Umani

La procedura di restore è l'operazione di ripristino dei file da un archivio, da dischi o nastri o altre unità di memoria di massa alle loro posizioni originali sul disco rigido del computer e può essere vista come l'operazione inversa al backup.
Ripristino totale o "Bare Metal"

Il "ripristino totale o bare metal" è il modo con il quale gli amministratori descrivono il processo di ripristino di un backup completo del sistema, su di un computer sprovvisto di dati di alcun genere (senza sistema operativo, applicazioni ecc.)

Il metodo più veloce per poter affrontare la suddetta problematica è quello di effettuare una reinstallazione totale del sistema, seguita dal processo di ripristino dei dati. Innanzitutto occorrerà configurare il nuovo hardware in caso di rottura o addirittura sostituzione della macchina (Configurazione RAID, Installazione nuove parti, Formattazione HD). Dopodichè dovrà essere reinstallato il sistema operativo della macchina tramite gli appositi dischi di ripristino precedentemente creati o comunque scaricabili dal sito del produttore. Una volta implementato il sistema operativo e configurato correttamente, dovranno essere installati i software applicativi presenti in precedenza a seconda dell'utilizzo della macchina. Infine dovranno essere ripristinate le basi dati dall'ultimo backup disponibile tramite l'apposito software di ripristino Tivoli Storage Manager (Vedi paragrafo Come Effettuare il restore con TSM).

Le operazioni di ripristino dei dati dovranno essere effettuate soltanto da personale autorizzato.

Il personale dell'Area Sistemi Informativi risulta essere l'incaricato a svolgere la procedura di ripristino dei dati.

Il tempo di Restore dei dati, per un ripristino totale della macchina, può variare a seconda delle operazioni da svolgere e solitamente può essere effettuato tra gli 1 e i 5 giorni.

Ripristino parziale

Il ripristino parziale è il modo con il quale gli amministratori descrivono il processo di ripristino di file e directory cancellati erroneamente da sistema.

Il metodo più veloce per poter affrontare la suddetta problematica è quella di ripristinare il file e le directory dall'ultimo backup disponibile tramite l'apposito software di ripristino Tivoli Storage Manager (Vedi paragrafo Come Effettuare il restore con TSM).

Le operazioni di ripristino dei dati dovranno essere effettuate soltanto da personale autorizzato.

Il personale dell'Area Sistemi Informativi risulta essere l'incaricato a svolgere la procedura di ripristino dei dati.

Il tempo di Restore dei dati, per un ripristino parziale, può variare a seconda delle dimensioni del file e delle directory e solitamente può essere effettuato nel giro di poche ore.

In caso di cancellazione accidentale dei dati sotto oggetto di backup da parte degli utenti, questi ultimi dovranno rivolgersi nel più breve tempo possibile al personale dell'Area Sistemi Informativi, che avvierà le procedure per il ripristino. Gli utenti dovranno compilare un modulo di richiesta di ripristino motivando l'evento (cancellazione involontaria, File Corrotto, etc.) che ha compromesso l'utilizzo del dato. Il modulo suddetto è presente in ISO come **EDP06 - Modulo di richiesta di ripristino dati**.

Come effettuare il Restore con IBM Tivoli Storage Manager

Ci sono più modi per effettuare il ripristino dei dati tramite il software TSM. Uno di questi è l'utilizzo dell'Interfaccia grafica per l'utente (GUI). Tramite questa interfaccia è possibile ripristinare file specifici, un gruppo di file con nomi simili o directory. È possibile individuare i file da ripristinare mediante la ricerca e il filtraggio. Il filtraggio visualizza solo i file che soddisfano i criteri relativi all'operazione di ripristino. I file che non soddisfano i criteri di filtraggio non vengono visualizzati. L'elaborazione del filtro ricerca i file di una determinata directory, ma non include le sottodirectory. Per

ripristinare i file e le directory utilizzando la GUI del client, si dovrà procedere nel seguente modo:

1. Fare clic su **Restore** sulla finestra principale. Viene visualizzata la finestra Restore.
2. Espandere la struttura della directory facendo clic sul segno più **(+)** o sull'icona della cartella accanto all'oggetto nella struttura. Selezionare l'oggetto da ripristinare. Per ricercare o filtrare i file, fare clic sull'icona **Find Files** dalla barra degli strumenti.
3. Per modificare determinate opzioni di ripristino, fare clic sul pulsante **Options**. Le opzioni modificate risultano disponibili solo durante la sessione corrente.
4. Fare clic su **Restore**. Viene visualizzata la finestra Destinazione ripristino. Immettere le informazioni appropriate.
5. Fare clic su **Restore**. La finestra Elenco attività mostra lo stato di elaborazione del ripristino.

Per ripristinare una versione di backup inattiva, è necessario visualizzare sia la versione attiva che quella inattiva facendo clic sul menu **View -> Display active/inactive files**. Per visualizzare solo le versioni attive (predefinite), fare clic sul menu **View -> Display active files only**. Se si tenta di ripristinare contemporaneamente sia una versione attiva che disattiva, viene ripristinata solo la versione attiva.

Nella riga comandi di Tivoli Storage Manager, utilizzare l'opzione ***inactive*** per visualizzare sia gli oggetti attivi che quelli inattivi.

Pianificazione Piano di Ripristino

Per fare in modo di testare la corretta validità dei backup è stato pianificato annualmente un piano di ripristino. Questo piano consiste nel prelevare a campione una parte delle basi dati backuppate ed effettuare il ripristino parziale o totale su delle macchine di test in precedenza configurate con il sistema operativo (Ex. Macchine virtuali di Test). Da qui si procede con l'installazione del software base (software applicativi) e successivamente al Restore della base dati. Alla fine dell'operazione verrà compilato il modulo **EDP06 - Modulo di richiesta di ripristino dati**, presente in ISO, che verrà utilizzato come verbale del Piano di Ripristino. Nel caso di successo il piano di ripristino verrà ripianificato per l'anno successivo, in caso di insuccesso dovranno

essere riviste immediatamente le procedure di backup e ripianificato il piano di ripristino nell'arco di due settimane. Il piano di ripristino dovrà essere tentato finchè quest'ultimo non è andato a buon fine. Il Piano di Ripristino è stato pianificato per il mese di Agosto/Settembre.

Tale procedura è documentata e tenuta aggiornata nell'allegato "Sistemi informativi - PO01 - Procedure di Backup e Ripristino - v03".
Lo storage dedicato ai backup è basato su sistema RAID 5 garantendo quindi la resilienza dal punto di vista informatico come richiesto dal Regolamento Europeo.

8.2.8 Criteri e modalità in caso di dismissione hardware

Nel caso in cui si presenti la necessità di riutilizzare o dismettere componenti hardware contenenti dati personali verrà seguita la procedura indicata nell' "Allegato Dismissione Hardware".

8.2.9 Registri per i controlli periodici

Come "Allegato Controlli periodici" si intende un file di excel, aggiornato periodicamente (come indicato all'interno del file) che contiene l'esito dei controlli, effettuati da un incaricato del reparto IT, alla ricerca di eventuali anomalie e/o violazioni dati. Questo file verrà azzerato all'inizio di ogni anno solare e le vecchie versioni saranno sottoposte a backup e conservate per 12 mesi.
Il file contiene il registro dei seguenti controlli:

- Controllo file di log delle VPN
- Controllo manuale dei backup dislocati
- Controllo manuale dei backup
- Controllo fisico della sala CED
- Controllo dei file log del firewall
- Controllo file di log del server DHCP
- Controllo file di log dei/del NAS o storage di rete
- Controllo delle utenze non più attive da 6 mesi

- Controllo sicurezza sito internet
- Controllo aggiornamenti e funzionamento antivirus
- Ricerca di file protetti da copyright all'interno della LAN

Tutti questi controlli vengono effettuati per verificare che il sistema, la gestione e il mantenimento delle risorse IT siano sempre efficienti ed efficaci alla ricerca di eventuali data breach o violazioni dati.

Inoltre è stata implementata l'analisi dei file log accesso tramite un sistema Privacy-C Amministratori di Sistema della società Compet-e che aiuta la predisposizione di report anche in modo automatizzato.

8.3 Valutazione Impatto del rischio

La misura di sicurezza avente ad oggetto la valutazione d'impatto del rischio (DPIA) è disciplinata dall'art 35 del Regolamento n. 679/16.

"Per potenziare il rispetto del presente regolamento qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento è responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio. L'esito della valutazione deve essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento. Laddove la valutazione d'impatto sulla protezione dei dati indichi che i trattamenti presentino un rischio elevato che il titolare del trattamento non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, prima del trattamento si dovrebbe consultare l'autorità di controllo"9.

Una DPIA è un processo volto a descrivere il trattamento, valutare la necessità e la proporzionalità di una lavorazione e per aiutare a gestire i rischi per i diritti e le libertà delle persone fisiche risultanti dal trattamento di dati personali.

8.3.1 Soggetti coinvolti

I soggetti obbligati ad assicurare la redazione della valutazione d'impatto sono il titolare ed il responsabile.

[9] Considerando n. 84

Il DPO, ed eventualmente l'ufficio competente, forniscono supporto al Titolare per lo svolgimento della DPIA.
Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

8.3.2 Tempi e casi in cui è prevista la DPIA

La valutazione d'impatto del rischio va fatta prima di iniziare il trattamento al fine di verificare la particolare probabilità e gravità del rischio.
La DPIA è obbligatoria in caso di:

a. uso di nuove tecnologie (art. 35.1);
b. 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 (art. 35.3);;
c. 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 (art. 35.3);
d. la sorveglianza sistematica su larga scala di una zona accessibile al pubblico (art. 35.3); .

Nei casi in cui non sia chiaro se sia necessaria una DPIA, il WP29 raccomanda che una VIP venga eseguita. Ed invero la DPIA, rammenta il WP29 è uno strumento utile per aiutare il titolare del trattamento a conformarsi alla normativa sulla protezione dei dati.
L'art. 35, par. 1 prevede che "Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi".

Per cercare di fornire qualche certezza in merito ai trattamenti "suscettibili di provocare un rischio elevato", il WP 29 ritiene che dovrebbero essere considerati i seguenti criteri:

1. "**La valutazione o l'assegnazione di un punteggio,** incluse la profilazione e la predizione, in particolare dagli "aspetti concernenti le prestazioni della persona interessata al lavoro, la situazione economica, la salute, le preferenze o interessi

personali, l'affidabilità o il comportamento, la posizione o gli spostamenti" (punti 71 e 91). Esempi di questo genere potrebbero includere una banca che scremi i propri clienti tramite una banca dati di riferimento del credito, o di una società di biotecnologie che offre test genetici direttamente ai consumatori, al fine di valutare e prevedere i rischi di malattia / salute, o una società di costruzione di profili comportamentali o di marketing in base all'utilizzo o alla navigazione sul suo sito web.

2. **Decisioni automatiche con effetti giuridici o similmente significativi**: elaborazione che mira a prendere decisioni su soggetti interessati e che produce "effetti giuridici riguardanti la persona fisica" o che "allo stesso modo sia determinante per la persona fisica" (articolo 35 (3) (a)). Ad esempio, il trattamento può comportare l'esclusione o la discriminazione di singoli. Elaborazione con poco o nessun effetto su individui non corrisponde a questo criterio specifico. Ulteriori spiegazioni su queste nozioni saranno fornite nelle prossime linee guida del WP29 in materia di Profilazione.

3. **Controllo sistematico**: trattamento utilizzato per osservare, monitorare o controllare soggetti interessati, inclusi i dati raccolti attraverso "un controllo sistematico di una zona accessibile al pubblico" (articolo 35 (3) (c)). Questo tipo di monitoraggio è considerato perché i dati personali possono essere raccolti in circostanze in cui gli interessati potrebbero non essere a conoscenza di chi sta raccogliendo i loro dati e di come saranno utilizzati. Inoltre, potrebbe essere impossibile per le persone evitare di essere oggetto di tale trattamento in spazi pubblici abituali (o accessibili al pubblico).

4. **Dati Sensibili**: questo include le categorie particolari di dati ai sensi dell'articolo 9 (per esempio, informazioni sulle opinioni politiche degli individui), nonché i dati personali relativi alle condanne penali o ai reati. Un esempio sarebbe il mantenimento complessivo delle cartelle dei pazienti in un ospedale o un investigatore privato che conserva i dettagli sui trasgressori. Questo criterio include anche i dati che possono più in generale essere considerati come aggravanti del possibile rischio per i diritti e le libertà delle persone, come i dati di comunicazione elettronica, i dati relativi all'ubicazione, i dati finanziari (che potrebbero essere utilizzate per le frodi nei pagamenti). A questo proposito, può essere rilevante definire se i dati siano stati resi pubblici dalla persona interessata o da terze parti. Il

fatto che i dati personali siano disponibili al pubblico può essere considerato come un fattore nel valutare se ci si aspetta che i dati siano ulteriormente utilizzati per determinati scopi. Questo criterio può anche includere informazioni elaborate da una persona fisica per l'esercizio di attività di carattere esclusivamente personale o domestico (come servizi informatici di storage per la gestione dei documenti personali, servizi di posta elettronica, diari, e-reader dotato di caratteristiche per prendere appunti, e varie applicazioni con credenziali che possono contenere dati sensibili), la cui comunicazione o elaborazione per scopi diversi da attività domestiche può essere percepito come molto invadente.

5. **I dati elaborati su larga scala**: il GDPR non definisce cosa costituisca larga scala, anche se il considerando 91 fornisce alcune indicazioni. In ogni caso, il WP29 raccomanda che i seguenti fattori, in particolare, siano considerati per determinare se il trattamento è effettuato su larga scala]:

6. **il numero di persone interessate,** come numero specifico o come percentuale della popolazione di riferimento;

7. **il volume dei dati e / o la gamma di diversi elementi di dati** in corso di elaborazione;

8. **la durata, o la permanenza, dell'attività di elaborazione dati;**

9. **l'estensione geografica** delle attività di elaborazione.

10. **Set di dati che sono stati abbinati o combinati**, ad esempio provenienti da due o più operazioni di trattamento effettuati per scopi diversi e / o da altri titolari in modo tale da superare le ragionevoli aspettative dell'interessato.

11. **I dati relativi interessati vulnerabili** (considerando 75): il trattamento di questo tipo di dati può richiedere una DPIA a causa del maggiore squilibrio di potere tra la persona e il titolare, cioè l'individuo non può essere in grado di consentire, od opporsi, al trattamento dei propri dati. Ad esempio, i dipendenti incontrerebbero spesso serie difficoltà nell'opporsi al trattamento effettuato dal datore di lavoro, quando legato alla gestione delle risorse umane. Allo stesso modo, i bambini possono essere considerati come non in grado di opporsi o acconsentire al trattamento dei propri dati consapevolmente e in maniera ponderata. Ciò riguarda anche il segmento più vulnerabile della popolazione che necessita di protezione

speciale, come, ad esempio, i malati mentali, i richiedenti asilo, o gli anziani, un paziente, o in ogni caso in cui può essere identificato uno squilibrio nel rapporto tra la posizione della persona interessata e il titolare.

12. **L'uso innovativo o l'applicazione di soluzioni tecnologiche o organizzative**,

    Il GDPR mette in chiaro (articolo 35 (1) e considerando 89 e 91) che l'uso di una nuova tecnologia può innescare la necessità di effettuare una DPIA. Questo perché l'uso di tale tecnologia può comportare nuove forme di raccolta e di uso dei dati, possibilmente con un rischio elevato per i diritti e le libertà degli individui. In effetti, le conseguenze personali e sociali della diffusione di una nuova tecnologia potrebbero essere sconosciute. Una DPIA aiuterà il titolare del trattamento a capire e trattare tali rischi. Ad esempio, alcune applicazioni di "Internet delle cose" potrebbero avere un impatto significativo sulla vita quotidiana e sulla privacy degli individui; e quindi richiedono una DPIA oppure combinando l'uso di impronte digitali e il riconoscimento del volto per un migliore controllo di accesso fisico, ecc.

13. **Il trasferimento dei dati attraverso i confini al di fuori dell'Unione europea** (considerando 116), prendendo in considerazione, tra gli altri, il Paese o i paesi di destinazione prevista, la possibilità di ulteriori trasferimenti o la probabilità di trasferimenti basati su deroghe per situazioni specifiche stabilite dal GDPR.

14. Quando l'elaborazione in sé **"impedisce agli interessati di esercitare un diritto o utilizzare un servizio o un contratto**" (articolo 22 e punto 91). Questo include lavorazioni eseguite in un'area pubblica che le persone che passano non possono evitare, o trattamenti che mirano a consentire, modificare o rifiutare l'accesso delle persone interessate a un servizio o alla stipula di un contratto. Un esempio di questo è quando una banca scremi i propri clienti tramite una banca dati di riferimento del credito al fine di decidere se offrire loro un prestito".

Il WP29 ritiene che qualora il trattamento presenti due o più criteri tra quelli sopra elencati sussista un rischio elevato per i diritti e le libertà delle persone, e quindi richieda una DPIA. Come regola generale, un'operazione di elaborazione che includa meno di due criteri può non richiedere una DPIA per il minore livello di rischio e operazioni di trattamento.

La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

Dall'analisi dei trattamenti, risulta come le operazioni di trattamento che richiederebbero una DPIA siano in capo ai Comuni, pertanto, si attendono determinazioni da essi, tuttavia In via precauzionale, in accordo con Pegaso 03 srl si può valutare di effettuare DPIA in merito al trattamento dati: gestione tari: e numero verde .

8.3.3 Consultazione

L'art 35 par. 9 prevede la possibilità per il titolare del trattamento di raccogliere le opinioni degli interessati o dei loro rappresentanti sul trattamento.

Il Wp 29 Il WP29 ritiene che:

- tali opinioni potrebbero essere ricercate attraverso una varietà di mezzi, a seconda del contesto (ad esempio, uno studio interno o esterno legato alla finalità e modalità dell'operazione di elaborazione, una domanda formale ai rappresentanti del personale, alle associazioni di categoria o ai sindacati o un sondaggio inviato ai futuri clienti del titolare del trattamento);
- se la decisione finale del titolare del trattamento differisce dal punto di vista degli interessati, i motivi per andare avanti o meno devono essere documentati;
- il titolare deve anche documentare le ragioni per non indagare il punto di vista delle persone interessate, se si decide che questo non è appropriato.

8.3.4 Contenuto della valutazione

La valutazione d'impatto ai sensi dell'art 35 par 7 deve contenere

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;
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.

8.3.5 La consultazione preventiva ed il suo contenuto

Ogni qualvolta dalla valutazione d'impatto emerga l'esistenza di un rischio elevato per i diritti e le libertà delle persone fisiche e che esso non possa essere attenuato mediante l'uso delle tecnologie a disposizione e per gli elevati costi di attuazione è necessario consultare l'autorità di controllo prima di procedere al trattamento.

La Consultazione ai sensi dell'art 36 par 3 deve prevedere:

a. ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;
b. le finalità e i mezzi del trattamento previsto;
c. le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento;
d. ove applicabile, i dati di contatto del titolare della protezione dei dati;
e. la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35;
f. ogni altra informazione richiesta dall'autorità di controllo.

L'Autorità di controllo pronuncia, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e ove applicabile al responsabile e può prevedere delle prescrizioni..

Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto.

L'Autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.

9. DATA BREACH

Per violazione dei dati personali (in seguito “data breach”) si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati da **COVAR 14**.

Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo.

Il Covar 14 tuttavia in qualità di Responsabile del trattamento è obbligato a sua volta a ad informare il Titolare (Comune) entro 72 ore dalla notifica della violazione, anche se a comunicarlo a Covar14 è la società Pegaso 03 srl.

I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:

- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione d’identità;
- perdite finanziarie, danno economico o sociale.
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati “elevati” quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

La notifica deve avere il contenuto minimo previsto dall'art. 33 RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.

Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del RGPD.

Il codice distingue tra la notificazione eseguita nei confronti dell'Autorità di controllo (art.33) da quella effettuata nei confronti dell'interessato (art.34).

9.1 Notificazione all'autorità di controllo

Il Regolamento UE Privacy, in caso di data breach, impone a tutti i Titolari del Trattamento (indipendentemente da dimensione, fatturato e settore di intervento) la notificazione privacy della violazione dei dati personali al Garante per la Protezione dei Dati Personali entro 72 ore dal momento in cui si è venuti a conoscenza del fatto.

Nel caso, il titolare del trattamento provveda alla notificazione del data breach oltre il termine di 72 ore, dovrà motivare al Garante Privacy le ragioni del ritardo, al fine di non incorrere nelle sanzioni previste dal Regolamento Europeo Privacy.

La notifica deve contenere:

a) **descrivere la natura della violazione dei dati personali compresi**, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) **comunicare il nome e i dati di contatto** del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) **descrivere le probabili conseguenze** della violazione dei dati personali;
d) **descrivere le misure adottate** o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora non sia possibile fornire le informazioni contestualmente, possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Il titolare del trattamento è esentato dall'effettuare la notifica solo se è in grado di dimostrare al Garante Privacy che la violazione dei dati personali non presenta rischi per i diritti e per le libertà fondamentali delle persone fisiche interessate.

In ogni caso, il titolare del trattamento ai sensi dell'art 33 paragrafo 5 dovrà **documentare le violazioni** di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati.

9.2 Notificazione all'interessato

In tutti i casi in cui la violazione dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà fondamentali degli interessati, il Regolamento obbliga il titolare del trattamento a comunicare l'avvenuto data breach anche a ciascun interessato al fine di consentirgli di adottare idonee precauzioni volte a ridurre al minimo il potenziale danno derivante dalla violazione dei suoi dati personali.

La comunicazione del data breach all'interessato deve essere effettuata utilizzando un linguaggio semplice e chiaro e deve avere come contenuto minimo:

a. comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
b. descrivere le probabili conseguenze della violazione dei dati personali;

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

Il Titolare del trattamento è esentato dall'effettuare la comunicazione della violazione dati personali all'interessato solo qualora sia soddisfatta una delle seguenti condizioni:

a. il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b. il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
c. detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o meno.
Per la gestione del Data Breach viene composto un Team di crisi costituito da:

- DPO nominato
- Data Manager Area Amministrazione Generale e Finanziaria:
- Privacy Officer Area Partecipate, Contenzioso Tributario e Gestione Personale:
- Privacy Officer it/Amministratore di sistema: IT di Pegaso 03 srl

Fanno parte del Team anche altre funzioni, di volta in volta coinvolte in base all'evento (es. altri Privacy officer, responsabile esterno o subresponsabile)
La procedura Data Breach fornisce le indicazioni per la gestione della violazione dei dati.

10. MISURE DI CONTROLLO

10.1 Misure edilizie

10.1.1 Accesso ai locali

L'accesso ai locali di **COVAR 14** è controllato mediante videocitofono.
Gli accessi alle parti comuni dell'edificio devono essere chiusi (a chiave nel caso delle porte) negli orari in cui **COVAR 14** è chiuso al pubblico. Negli orari di apertura al pubblico/lavoro, nessun dato personale deve essere posto in vista, o deve essere facilmente accessibile o riconoscibile a chiunque.

Vediamo ora le disposizioni riguardanti specifici locali:

- **Uffici**

L'accesso agli Uffici è strettamente controllato da parte degli Autorizzati al trattamento che effettuano trattamenti di dati personali. Durante il normale orario di apertura degli Uffici, l'accesso ai dati è controllato dai rispettivi autorizzati al trattamento e qualora, per motivi diversi, un Ufficio rimanga temporaneamente vuoto, l'autorizzato al trattamento è obbligato a chiudere a chiave la porta d'accesso dello stesso e custodire la copia di chiavi che ne permettono l'apertura (ovvero consegnarla al collega o ad altro soggetto che comunque abbia diritto ad espletare la propria attività nel medesimo Ufficio).

In ogni caso, ciascun autorizzato al trattamento deve rendere i dati personali specificamente trattati non consultabili o visibili da parte di eventuali terzi che abbiano diritto ad accedere all'Ufficio né al collega che stia svolgendo il proprio lavoro nel medesimo locale. I terzi estranei a **COVAR 14** che possono accedere agli Uffici negli orari di apertura e/o di chiusura sono espressamente determinati in apposite autorizzazioni/contratti loro conferiti, nei quali sono indicate le responsabilità loro riferite, quale ad esempio il personale di pulizia.

Tutti gli autorizzati al trattamento devono provvedere a non lasciare mai, in loro assenza, porte e finestre dei rispettivi Uffici aperte. Gli accessi specifici (cassetti, armadi, ecc.) vanno chiusi a chiave sempre, le porte solo in assenza degli addetti dai rispettivi Uffici. Tutti i dati particolari contenuti su documenti cartacei devono sempre essere conservati dentro armadi o contenitori chiusi a chiave.

- **Locali archivio**

Gli archivi correnti devono essere chiusi a chiave ed i dati conservati devono essere riposti in modo organizzato e sistematico, salvo che non rivestano più alcuna utilità per l'attività ordinaria di trattamento.

- **Sicurezza archivi cartacei**

Si ritiene fondamentale evidenziare le istruzioni al trattamento riguardanti la complessiva attività di **COVAR 14**, la cui applicazione pratica risulta essere di vitale importanza per la concreta applicazione del presente Modello Organizzativo. In particolare, tutte le informazioni riportate su documenti cartacei, delle quali si abbia effettiva esigenza di consultazione, devono essere prelevate e detenute in base alla loro attinenza e pertinenza con il trattamento richiesto.

Gli archivi sono ad accesso selezionato, cioè è possibile ricercare ed estrarre esclusivamente i dati necessari per il trattamento. Se si tratta di dati particolari o relativi a condanne penali e reati, ai sensi degli art. 9 e 10 del GDPR 679/2016, gli autorizzati al trattamento devono utilizzare esclusivamente i dati strettamente necessari allo svolgimento delle proprie mansioni ed immediatamente restituirli al termine delle operazioni.

I dati particolari o relativi a condanne penali e reati, così come sopra definiti, devono essere conservati dentro contenitori muniti di serratura. Se una o più informazioni devono rimanere a disposizione per un trattamento prolungato o continuo, l'incaricato deve essere sempre presente nel locale ove avviene il trattamento ed essere in grado di impedire a terzi di vedere la documentazione in uso. Nel caso in cui sia indispensabile l'accesso al locale da parte di terzi, l'autorizzato al trattamento provvede preventivamente a riporre tutti i dati personali in consultazione nei relativi siti protetti.

Tutti i soggetti, interni o esterni all'ente, che possono accedere all'edificio o anche ai dati cartacei sono muniti di esplicita autorizzazione, recante in dettaglio le regole per il corretto trattamento dei dati e/o i limiti e le responsabilità connesse al loro diritto di accesso. Tali autorizzazioni sono periodicamente controllate, al fine di verificare la loro osservanza ed adeguatezza alle condizioni di espletamento dei servizi ed in relazione alle motivazioni per le quali sono state assegnate.

Il dipendente ha l'obbligo di:

- evitare che persone non autorizzate possano leggere, copiare o comunque impossessarsi dei dati personali in sua custodia

- restituire o distruggere gli atti e i documenti contenenti dati personali al termine delle operazioni affidategli.

Il contenuto degli armadi è accessibile al solo dipendente.

Gli armadi devono essere chiusi quando il dipendente abbandona il proprio ufficio**.**

- **Archivio documenti dei dipendenti**

I documenti dei dipendenti, contenenti dati sensibili e personali, sono archiviati in armadi chiusi gestiti dall'ufficio personale che li tratta.
All'atto dell'assunzione ad ogni dipendente viene data l'informativa. I certificati di Malattia vengono comunicati direttamente tramite il portale INPS con il codice assegnato dal medico Curante.
Gli altri documenti sono trattati dall'ufficio personale e COVAR 14essi alla società che elabora gli stipendi quanto necessario. Anche in questo caso i documenti sono archiviati nella cartella del dipendente.

- **Archivio del casellario giudiziario**

La fotocopia del casellario giudiziario e carichi pendenti, può essere conservata al massimo per 6 mesi (periodo di validità dell'atto) e poi deve essere distrutto.

- Sull'utilizzo degli strumenti informatici si rinvia al Regolamento disposto da **COVAR 14** e approvato con delibera di cda

- **Codice di allarme**

Il codice dell'allarme e la procedura da seguire per attivarlo/disattivarlo, nonché per segnalare guasti e rimediare a errori è stata comunicata al personale mediante formazione. L'allarme è collegato ad una azienda che effettua servizio di sorveglianza.

10.3 Applicazione normativa D.lgs 81/2008

COVAR 14 applica la normativa sulla sicurezza dei luoghi di lavoro e la normativa sul fumo.

Sono presenti in sede le funzioni di: Responsabile della sicurezza e viene fatta formazione sulla normativa della sicurezza e primo intervento.

Sono attivi gli estintori, soggetti a manutenzione semestrale.

Tutto il personale è regolarmente aggiornato a cura del Responsabile della sicurezza e le prove di emergenza ed evacuazione sono annualmente eseguite.

11 MISURE PER IL PERSONALE

11.1 Procedura di selezione ed ingresso dei collaboratori

La necessità di introdurre un nuovo dipendente è una attività a carico dell'ufficio personale che definisce il profilo del dipendente. E' in capo al titolare la ricerca e la selezione del personale.

1. l'ufficio personale, una volta che il dipendente è stato individuato, procede al disbrigo delle pratiche amministrative in particolare:

- comunica all'ADS l'introduzione del nuovo dipendente, il ruolo ricoperto e la durata dell'incarico (a tempo determinato o indeterminato) affinché, quest'ultimo possa provvedere a predisporre la postazione IT con i privilegi e gli accessi congruenti alla posizione ricoperta;
- comunica alla funzione preposta l'introduzione del dipendente, affinché, possa provvedere a: fornirgli gli strumenti di ausilio all' attività (cellulare, chiavi, ecc.);
- comunica al Data Manager di riferimento;
- organizza, la formazione in materia di salute e sicurezza, privacy ed altra formazione necessaria per l'introduzione del nuovo dipendente. La formazione è registrata nel registro formazione
- fornisce al dipendente le informazioni relative agli aspetti amministrativi (richiesta ferie, permessi, ecc.);
- organizza la presentazione dell'organigramma, della struttura e dei colleghi;

2. La funzione responsabile dell'ufficio in cui il dipendente svolgerà la sua mansione si occupa di:

- illustrare il lavoro da svolgere, l'organizzazione della intranet aziendale, le modalità ed i criteri di archiviazione e naming dei file e le procedure relative al ruolo.

11.1.1 Consegna documentazione privacy dipendenti

Al dipendente viene allegata la seguente documentazione:

- nomina Privacy Officer/autorizzato al trattamento ed istruzioni operative
- consegna informativa al dipendente
- nomina di amministratore di sistema

- regolamento aziendale

11.2.1 Regolamento aziendale

Per tutti i dipendenti/collaboratori che hanno accesso a dati personali o ne eseguono l'elaborazione valgono le disposizioni contenute nel Regolamento Europeo 679/2016 in materia di protezione dei dati personali.

Per impedire che il personale entri inutilmente in conflitto con le disposizioni della legge, **COVAR 14** consegna ai propri dipendenti e collaboratori operanti in sede il "Regolamento aziendale che regolamenta le disposizioni in merito all'accesso e all'impiego dei mezzi informatici.

Il medesimo regolamento deve essere sottoscritto da chiunque abbia accesso autorizzato al sistema informatico, anche temporaneo (ad esempio collaboratori occasionali, stagisti …), in qualità di "autorizzato al trattamento".

11.3 Formazione

La formazione costituisce, un prerequisito per potere operare all'interno delle organizzazioni, imprese. Essa dovrebbe, alla luce dell'impianto del Regolamento, presentare un taglio interdisciplinare (con sessioni sia informatiche sia giuridiche sia sui profili organizzativi dell'Ente o Società) e riguardare tutti i soggetti.

La formazione è finalizzata ad illustrare i rischi generali e specifici dei trattamenti di dati, le misure organizzative, tecniche ed informatiche adottate, nonché le responsabilità e le sanzioni, in particolare:

- sui rischi che incombono sui dati
- sulle misure per prevenire eventi dannosi
- sulla disciplina sulla protezione dei dati più rilevanti in rapporto alle rispettive attività
- sulle responsabilità che ne derivano
- sulle modalità per aggiornarsi sulle misure minime adottate da **COVAR 14**

La formazione costituisce, pertanto, una misura di sicurezza per le organizzazioni, un onere a carico del titolare, un diritto e dovere per i dipendenti e i collaboratori.

COVAR 14 pertanto, ha previsto

- un registro della formazione;
- prove finali
- individuato un test finale ulteriore in caso di mancato superamento un percorso formativo alternativo, in caso di mancato superamento del test finale, ed un nuovo esame di verifica;
- sessioni di aggiornamento alla luce delle modifiche normative, organizzative e tecniche;

Gli autorizzati per il trattamento dei dati interni di **COVAR 14** sono individuati tra risorse dotate di adeguata esperienza, capacità ed affidabilità in base alle esigenze di trattamento dei dati presenti nella organizzazione.

Il Titolare del trattamento completa inoltre la formazione del personale relativamente alle modalità di gestione del sistema informatico e, se necessario, del software applicativo, in base al livello di competenza delle risorse.

11.3.1 Formazione iniziale

Il Titolare del trattamento prevede per ogni nuova risorsa da inserire in organico un modulo dedicato al tema della protezione dei dati personali all'interno del programma di formazione iniziale, con consegna e illustrazione delle indicazioni in merito all'applicazione del Regolamento Europeo 679/2016; ciò avviene, in particolare con la consegna della nomina come incaricato.

Deve inoltre essere effettuata, se necessario, un'azione formativa sulle modalità di gestione del sistema informatico e, se necessario in base alla valutazione iniziale delle competenze informatiche della nuova risorsa, un'ulteriore azione formativa relativa al software applicato.

Infine, all'atto dell'avvio del rapporto di lavoro con un dipendente l'ufficio personale comunica tramite la consegna del Regolamento aziendale le regole in merito all'uso dei mezzi informatici.

11.3.2 Formazione continua

COVAR 14, all'interno del piano annuale di formazione continua delle risorse, ha ritenuto di primaria importanza il tema della Protezione dei dati personali, su cui ha impostato il programma di formazione collettiva per tutte le risorse in organico.

Per gli anni successivi, in occasione degli aggiornamenti annuali del MOP, il Titolare del trattamento, nel rendere noto il nuovo testo, organizzerà, se necessario ed in relazione alla rilevanza delle variazioni intervenute, attività formative per segnalare le modifiche e innovazioni intervenute in materia di protezione dei dati personali e di gestione del sistema informatico. Ulteriore formazione, in materia di privacy, verrà pianificata ed eseguita a seguito dell'introduzione del Regolamento Europeo sul trattamento dei dati.

Nel caso dovessero intervenire nel corso dell'anno modifiche o innovazioni tali da necessitare un aggiornamento urgente di tutte le risorse il Titolare del trattamento provvederà alla organizzazione delle attività formative secondo le esigenze.

11.4 Procedura di dimissione

Nel caso di dimissione di un dipendente si procede a

- archiviare la documentazione del dipendente;
- comunicare all'ADS le dimissioni del dipendente affinché, quest'ultimo possa provvedere a: disattivare la connessione da remoto del dipendente, reindirizzare la posta elettronica, recuperare la postazione;
- comunicare alla funzione preposta la dimissione del dipendente, affinché, possa provvedere al ritiro degli strumenti di ausilio alla attività (cellulare, chiavi, ecc.)
- disattivare l'account e prevedere una risposta automatica con l'indicazione della nuova mail a cui indirizzare il messaggio.

Si richiama integralmente il Regolamento aziendale per ogni aspetto riferito alla dismissione degli strumenti informatici da parte del dipendete.

12 DATA RETENTION EVENTUALE

COVAR 14 è in possesso di una grande quantità di informazioni importanti e fondamentali per il funzionamento dell'organizzazione, che coinvolgono anche dati personali, nonché dati sensibili e pertanto soggetti all'adempimento di particolari

soddisfacimenti. Questo paragrafo ha l'obiettivo di indicare la durata dei periodi di conservazione dei dati personali trattati nello svolgimento delle attività societarie del titolare del trattamento.

COVAR 14 fornisce ai soggetti incaricati ad effettuare le operazioni di trattamento una guida sulla conservazione dei vari tipi di dati che la stessa detiene. In particolare, è necessario bilanciare da un lato la necessità per **COVAR 14** di memorizzare le informazioni per adempiere agli obblighi di legge, nonché ai propri interessi, mentre dall'altro di eliminare i dati in modo sicuro quando non è più necessario conservarli.

La politica sulla conservazione dei dati concerne tutte le informazioni personali di cui è titolare **COVAR 14** quindi sia quelle memorizzate e conservate in maniera cartacea, sia quelle detenute in modalità informatica ed elettronica, sia quelle trasmesse per posta, cartacea e/o elettronica, che quelle comunicate oralmente, come tramite contatto telefonico.

Il documento dovrà applicarsi a tutto il personale e comunque a tutti gli utenti eventualmente autorizzati a trattare le informazioni personali di cui **COVAR 14** è titolare, al fine di garantire la continuità aziendale e per evitare violazioni di legge, o statutarie, o regolamentari, o contrattuali applicabili in materia. Il documento in parola è, quindi, utile a **COVAR 14** per impegnare tutti a proteggere i dati attraverso la conservazione in riferimento e secondo i principi di riservatezza, di integrità e di disponibilità richiesti dalla normativa.

La parte più complessa, tuttavia, rimane la scelta dei termini di conservazione dei singoli dati trattati da **COVAR 14** e quindi dei relativi documenti che li contengono. Le politiche inerenti i termini di conservazione non sempre sono stabiliti normativamente, al contrario per taluni trattamenti è necessario procedere ad un'attenta verifica che il risultato contemperi l'indubbio interesse aziendale a conservare i dati, con i principi fissati dal GDPR anche rispetto alle finalità di trattamento perseguite.

Si precisa da ultimo che i tempi di conservazione dei dati dei dati dovranno essere resi noti a tutto il personale.

12.1 Policy Data Retention

In relazione all Policy Data Retention, **COVAR 14** dispone di un Regolamento di Protocollo e di un massimario al quale si attiene per i tempi di conservazione della

documentazione, salvo particolari casi di ricorsi e connesse esigenze processuali, e casi di specifici adempimenti indicati in caso di nomina a . Responsabile del trattamento, nei limiti dei tempi regolamentati e comunque a tutela delle parti.

ALLEGATI

INDICE ALLEGATI

A) Allegati al MPO
Informative :
Informative alle utenze, informative del numero verde, informativa ai fornitori e ai clienti, informativa per la newsletter , policy sito, (pubblicati sul sito internet)
Altre informative:
Informativa consulenti, informative dipendenti, informativa visitatori, informativa stagisti, i informativa per assunzioni.

B) Registro dei trattamenti è un programma strutturato e gestito in capo alle Aree per competenze generali e implementato dall'Area Ammin Gen e finanziaria/ Segreteria;

C) Organigramma Privacy; Analisi dei rischi sett. 2018 allegati alla delibera di CdA n. 9 del 06 marzo 2019 ad oggetto: APPROVAZIONE DELLA STRUTTURA PRIVACY IN CONFORMITA' AL GDPR N. 16/679;

D) Nomina Privacy Officers e Data Manager
Nomina Privacy Officer amministratore di sistema
Nomina Responsabili del trattamento
Nomina soggetti autorizzati
Nomina Subresponsabili
Nomina COVAR 14 responsabile esterno come da delibera di CdA n. 9 del 06 marzo 2019 ad oggetto: APPROVAZIONE DELLA STRUTTURA PRIVACY IN CONFORMITA' AL GDPR N. 16/679 inseriti nel programma della privacy

E) Nomina Dpo delibera di CDA nomina esterna soggetta a modifiche periodiche

F) DPIA
Policy data breach e DPIA, Regolamento per l'utilizzo degli strumenti informatici allegati alla delibera di CDA che approva questo stesso documento (MOP)

G) Procedure ancora in corso di stesura da parte di Pegaso 03srl

Procedura server proxer (pag 42)
Procedure di Backup e Ripristino - v03(pag 42)
Procedura "VPN" (pag 48)
Procedura di Power-up/Shutdown" (pag 53)
Procedura di dismissione hardware (pag 54)
Procedura Controlli periodici (pag 60)
Procedura Dismissioni e Back up e ripristino

APPENDICE 1

Terminologia

1. Terminologia afferente al Regolamento Europeo 679/2016

Banca di dati:

> "qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti"

Comunicazione:

> "il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, del responsabile e degli autorizzati al trattamento, in qualunque forma, anche mediante la loro messa a disposizione o consultazione"

Dato personale:

> "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".

Dato/i Personale/i" "Categorie Particolari di Dati"

> "ogni Dato Personale idoneo a rivelare l'origine razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché 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 (anche detti "Dati Sensibili" ai sensi del D.lgs. 196/2003)".

Dati giudiziari:

> "ogni Dato Personale relativo a condanne penali e ai reati o a connesse misure di sicurezza ovvero relativo a provvedimenti giudiziari, sanzioni penali, o carichi pendenti, o la qualità dell'imputato o indagato ai sensi degli articoli 60 e 61 del Codice di Procedura Penale".

Diffusione:

> "il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione"

Autorizzati al trattamento:

"le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile e che agiscono sotto l'autorità del Titolare o del Responsabile ai sensi dell'art. 30 del Codice Privacy e dell'art. 29 del GDPR".

Interessato:

"la persona fisica, la persona giuridica, l'ente o l'associazione a cui si riferiscono i dati personali"

Responsabile:

"la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che tratta dati per conto del Titolare del trattamento dei Dati Personali".

Titolare:

"la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Ai fini del presente atto con il termine Titolare si intende COVAR 14"

Trattamento:

"qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trCOVAR 14issione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

2. Terminologia afferente al sistema informatico

Cookie:

I cookie consentono al Web Master di perfezionare l'offerta e al visitatore di interagire più rapidamente. ciononostante, i cookie godono di cattiva fama. Un cookie può ad esempio essere del tipo seguente:

www.ora.com FALSE I FALSE 946684799 ora-account 123

I cookie sono informazioni testuali, che vengono depositate in un file speciale sul disco rigido la workstation. I cookie non possono contenere alcun virus. Vi sono contenute le informazioni, di cui il Web Server ha bisogno per potervi servire meglio. I file dei cookie sono raramente di grandezza superiore a 3000 bytes e i cookie risalenti a più di 30 giorni vengono di regola cancellati automaticamente.

Esempio:

Se si inizia una ricerca presso uno dei grandi motori di ricerca, insieme al risultato arriva un cookie contenente le seguenti informazioni:

- Cosa è stato cercato
- Cosa è stato trovato
- Come si può proseguire la ricerca

Dominio:

Un nome o un indirizzo per minimo un computer o un intero gruppo di computer raggruppati dal punto di vista geografico, organizzativo o tematico (ad es. tutti i computer di COVAR 14 costituiscono il dominio www.atapspa.com)

E-Mail:

Abbreviazione per Electronic Mail (posta elettronica). Mediazione di messaggi e corrispondenza tramite reti di comunicazione disponibili in tutto il mondo.

Internet:

Rete mondiale di computer, strutturata in modo non gerarchico. È composta di diversi servizi, operanti secondo standard unificati. I servizi più noti sono E-Mail, FTP e WWW.

Intranet:

Rete chiusa di aziende o gruppi di aziende, che fa uso delle tecnologie di Internet.

Extranet:

Una intranet, in cui sono collegati i clienti, i fornitori e i partner, che comunicano tramite Internet utilizzando nomi utente e password predefiniti. L'intranet viene per così dire estesa in Internet, costituendo tutta via un'area protetta.

POLICY PRIVACY SITO

Covar 14 con sede in Carignano, Via Caglieri n. 3, in qualità di titolare del trattamento, intende informarLa in merito al trattamento dei suoi dati all'interno del sito web: www.covar14.it.

Il nostro obbiettivo è quello di garantire in qualsiasi momento la tutela dei Suoi dati personali. Le chiediamo, quindi, di leggere con attenzione l'Informativa sulla Privacy per sapere quali informazioni vengono raccolte e per quale scopo vengono utilizzate.

Il Regolamento Europeo privacy 2016/679 per dato personale intende qualsiasi informazione riguardante una persona fisica, identificata o identificabile. Una persona fisica identificabile è un soggetto che può essere identificato, in modo diretto o indiretto, tramite riferimento a identificativi quali nome, numero del documento d'identità, dati sulla sua ubicazione, identificativo online o uno o più fattori specifici dell'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di tale persona.

Non sono considerati personali i dati resi anonimi o in forma aggregata in modo da non consentire più l'identificazione della persona fisica specifica, nemmeno in combinazione con altre informazioni o in altri modi.

1) Tipi di informazioni raccolte

Di seguito sono elencate le attività che può svolgere sul sito e dalle quali la Società può acquisire Suoi dati personali, in particolare quando

1. A)CONTATTA IL TITOLARE DEL TRATTAMENTO PER PORRE DOMANDE

   Qualora intenda interloquire con Covar 14 mediante gli indirizzi mail contenuti alla voce " contatti" Covar 14 potrà acquisire suo indirizzo mail nonché eventualmente il suo nome e cognome che verranno trattati al solo fine di poterLe fornire un'esauriente risposta in merito a domande e/o osservazioni da Lei poste.

   La base giuridica di questo trattamento è l'esecuzione di un contratto e/o misure precontrattuali

2. B)PER ISCRIVERSI ALLA NEWSLETTER

   Qualora intenda ricevere informazioni in merito ai servizi offerti da Covar 14 potrà iscriversi alla News letter . Per tale trattamento è necessario che lei comunichi il suo indirizzo mail mediante l'apposito form. L'invio della news letter può avvenire solo con il suo consenso.

   Per di più si veda l'informativa redatta ad hoc per l'invio della news letter.

3. C)PER VALUTARE IL GRADO DI SODDISFACIMENTO DEL SERVIZIO OFFERTO DA COVAR 14
   I dati raccolti sono anonimi, pertanto non sono sottoposti alla disciplina del GDPR. Ed invero non viene né visualizzato né conservato l'indirizzo ip.

2) FINALITÀ DEL TRATTAMENTO

Tutte le informazioni raccolte sono trattate dal Titolare del trattamento:

1. per rispondere a sue domande/ suggerimenti;
2. per invio di informazioni riguardanti l'attività svolta da Covar 14
3. per valutare il gradimento del servizio

I suoi dati verranno trattati utilizzando strumenti manuali nonché strumenti informatici anche mediante l'inserimento di essi in banche dati, elenchi e liste idonei alla memorizzazione, gestione e trasmissione dei dati, nei modi e nei limiti necessari al perseguimento delle predette finalità.

I Suoi dati saranno trattati esclusivamente da persone autorizzate al trattamento.

3) NATURA DEL CONFERIMENTO DEI DATI E CONSEGUENZE DEL RIFIUTO

Il conferimento dei dati personali da parte Sua, è facoltativo per ciascuna delle finalità indicate al punto 2, tuttavia, l'eventuale mancato conferimento, comporterà, l'impossibilità di adempiere alle sue richieste.

L'attività di informazione mediante news letter sarà svolta solo in caso di suo consenso, che potrà da Lei essere revocato in ogni momento scrivendo a infoedatabreach@covar14.it

4) AMBITO DI COMUNICAZIONE – TRASFERIMENTO E DIFFUSIONE DEI DATI

I suoi dati personali, potranno essere comunicati a soggetti terzi, espressamente nominati responsabili del trattamento, in particolare a Società che gestiscono il sito web per il perseguimento delle finalità indicate e nei limiti previsti dalla relativa normativa.

Ai dati potrebbero accedere (per finalità di assistenza al sito, agli applicativi, alla rete informatiche e per la connettività) nostri tecnici incaricati o consulenti esterni nominati anch'essi responsabili del trattamento.

Infine, potranno essere comunicati ai soggetti legittimati ad accedervi in forza di disposizioni di legge, regolamenti, normative comunitarie. In ogni caso, i dati personali conferiti non saranno oggetto di diffusione.

5) SICUREZZA DEI VOSTRI DATI PERSONALI

Per proteggere i dati personali da accesso, divulgazione e modifica non autorizzati, abbiamo implementato dal punto di vista tecnico i sistemi di protezione e le relative misure di sicurezza che ne garantiscono la tutela. Queste misure di sicurezza vengono di volta in volta adattate per ottenere ogni volta un elevato livello di sicurezza. Tuttavia, tenete presente che, malgrado i nostri sforzi, nessuna misura di sicurezza è perfetta o impenetrabile. Inoltre, per aiutarci a mantenere alto il livello di sicurezza, vi chiediamo di custodire il vostro nome utente e password e di non svelarli a terzi.

6) DIRITTI DELL'INTERESSATO

La informiamo che il Regolamento europeo all'art. 15 e seg. Le conferisce i seguenti diritti :

- di accesso ossia la possibilità di ottenere la conferma che sia o meno in corso un trattamento e di acquisire informazioni in merito a: finalità di esso, categorie di dati personali in questione, destinatari dei dati in particolare se Paesi terzi, il periodo di conservazione ove possibile e le modalità del loro trattamento,
- alla rettifica e all'integrazione dei dati,
- alla cancellazione, ogniqualvolta i dati non siano necessari rispetto alle finalità oppure qualora decidesse di revocare il consenso o si opponesse al trattamento o ancora qualora i dati fossero trattati illecitamente;
- alla limitazione del trattamento nel caso in cui contesti l'esattezza dei dati personali per il periodo necessario per effettuare le relative verifiche, oppure il trattamento sia illecito, o qualora benchè il titolare del trattamento non abbia più bisogno dei suoi dati, lei richieda la conservazione per finalità giudiziarie;
- alla portabilità dei dati ad altro titolare, qualora il trattamento avvenga con mezzi automatizzati o sia basato sul consenso;
- di opporsi al trattamento dei propri dati personali in presenza di giustificati motivi o nel caso in cui gli stessi siano utilizzati per l'invio di materiale pubblicitario, di direct marketing o per il compimento di indagini di mercato;
- a proporre reclamo avanti all'Autorità.

Qualora decidesse di esercitare i diritti sopra descritti o in caso di violazione dei dati personali potrà contattare il titolare del trattamento al seguente indirizzo mail: infoedatabreach@unotetro.it

7) CONSERVAZIONE DEI DATI

Il Titolare del trattamento conserva e tratta i dati personali per il tempo necessario ad adempiere alle finalità indicate, in particolare per il servizio di news letter i dati vengono conservati fino a revoca del Suo consenso.

I dati raccolti per rispondere a sue domande o acquisiti mediante l'invio da parte sua di suggerimenti non saranno oggetto di conservazione;

I dati acquisiti durante la compilazione del questionario come già illustrati sono anonimi.

8) NEL CASO IN CUI SIATE DI ETÀ INFERIORE AI 16 anni

I nostri siti web sono riferiti a un'audience generalista e non sono rivolti ai minori. Non raccogliamo consapevolmente dati personali di utenti che in base alle leggi del loro Paese sono considerati minori.

9) TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento dei dati personali è Covar 14 con sede in Carignano, Via Caglieri n.3 qualora intendesse acquisire informazioni sulla protezione dei dati personali o segnalare violazioni riguardanti i dati personali potrà scrivere all'indirizzo di posta sopra indicato oppure all'indirizzo mail infoedatabreach@covar14.it

10) RESPONSABILE DELLA PROTEZIONE

La Società COVAR 14 ritenendo di primaria importanza la tutela dei dati personali degli interessati, ha nominato un responsabile della protezione dei dati (DPO) che potrà essere contattato scrivendo all'indirizzo mail dpo@covar14.it per ogni tematica riguardante la protezione dei dati personali.

SOCIETA' FORNITORI - CLIENTI

Informativa ex art 13 del Regolamento europeo n. 16/679

La Società Co.Va.R 14, con sede in Carignano (To), Via Cagliero 3I/3L, in qualità di Titolare del trattamento dei dati personali, con la presente desidera rendere un'adeguata informativa alle persone fisiche che operano in nome e per conto del fornitore ___/ della Società cliente/ Co.Va.R 14 in attività contrattuali o pre-contrattuali ai sensi dell'art. 13 d. lgs. 30 giugno 2003 n° 196 - "Codice in materia di protezione dei dati personali" e dell'art. 13 GDPR 679/16 – "Regolamento europeo sulla protezione dei dati personali".

1.Dati oggetto del trattamento

I dati personali trattati sono dati anagrafici e di contatto forniti o ricevuti dall'interessato in occasione di:

- visite o telefonate o email;
- contatti diretti ottenuti a seguito della partecipazione ad eventi, ecc.;
- richieste di informazioni commerciali, proposizione di offerte;
- richieste tramite il nostro sito internet o tramite il sito internet di fornitori, clienti, partner, altri soggetti
- trasmissioni e transazioni successive all'ordine di fornitura del servizio o del bene (fornito/acquistato)

2.Finalità del trattamento

I dati personali delle persone fisiche che operano in nome e per conto del fornitore/ della Società cliente Co.Va.R 14, e di altri soggetti sono trattati per:

- inoltrare comunicazioni con diversi mezzi di comunicazione (telefono, telefono cellulare, sms, email, fax, posta cartacea, ecc.);
- formulare richieste o evadere richieste pervenute;
- scambiare informazioni finalizzate all'esecuzione del rapporto contrattuale, ivi comprese le attività pre e post contrattuali, tra cui anche quelle di assistenza;
- esecuzione di obblighi previsti da leggi, regolamenti o dalla normativa comunitaria, nonché per ottemperare a provvedimenti emanati da pubbliche Autorità a ciò legittimate o da organi di vigilanza e di controllo a cui è soggetta la società (si pensi ad es. ad accertamenti di carattere tributario, ecc.).

L'interessato può rifiutarsi di conferire al Titolare i dati personali. Il conferimento dei dati personali è però necessario per una corretta ed efficiente gestione del rapporto contrattuale verso il fornitore, Società cliente Co.Va.R 14, e di altri soggetti coinvolti nelle attività del Titolare. Pertanto, un eventuale rifiuto al conferimento potrà compromettere in tutto o in parte il rapporto contrattuale stesso o le attività pre e post contrattuali.

3.Base giuridica

Il trattamento è necessario all'esecuzione di un contratto di cui ciascun soggetto è parte o all'esecuzione di misure precontrattuali o post contrattuali adottate su richiesta del fornitore/ della

Società cliente Co.Va.R 14, o della società ai sensi dell'art. 6.1, lett. b) del RGDP)., ovvero per l'adempimento di un obbligo legale ai sensi dell'art. 6.1, lett. c) del RGDP).

4.Modalità del trattamento

I dati degli interessati verranno trattati nel rispetto dei principi di liceità correttezza e trasparenza, utilizzando strumenti manuali o automatizzati anche mediante l'inserimento in banche dati, elenchi e liste idonei alla memorizzazione, gestione e trasmissione dei dati, nei modi e nei limiti necessari al perseguimento delle predette finalità.

La società ha previsto adeguate misure di sicurezza al fine di tutelare i dati delle persone fisiche che operano in nome e per conto dei fornitori, delle Società clienti.

I dati saranno trattati esclusivamente da persone autorizzate al trattamento in relazione alla finalità del trattamento.

La società non effettua processi decisionali automatizzati per le finalità indicate.

5.Destinatari dei dati

I dati personali trattati dal Titolare non saranno diffusi, ovvero non ne verrà data conoscenza a soggetti indeterminati, in nessuna possibile forma, inclusa quella della loro messa a disposizione o semplice consultazione. Potranno, invece, essere comunicati ai lavoratori del Titolare e ad alcuni soggetti esterni che con essi collaborano, sempre nel rispetto delle finalità indicate. In particolare, si tratta di dipendenti/collaboratori che, sulla base dei ruoli e delle mansioni lavorative espletate, sono stati legittimati a trattare i dati personali, formati a farlo nei limiti delle loro competenze ed in conformità alle istruzioni ad essi impartite dal Titolare. Potranno, inoltre, essere comunicati, nei limiti strettamente necessari, ai soggetti che per finalità di emissione dei nostri ordini o richieste di informazioni e preventivi o formulazioni di offerte, nostre prestazioni, debbano fornire/consegnare beni e/o eseguire/ricevere su nostro/vostro incarico prestazioni o servizi. Ai dati potrebbero accedere (per finalità di assistenza sugli applicativi SW, sulle rete informatiche e per la connettività) nostri tecnici incaricati o consulenti esterni o incaricati di società che forniscono tali servizi nominate responsabili del trattamento. Infine, potranno essere comunicati ai soggetti legittimati ad accedervi in forza di disposizioni di legge, regolamenti, normative comunitarie.

6.Trasferimento dei dati

Il Titolare del trattamento non trasferisce i dati personali in Paesi Terzi o a organizzazioni internazionali.

Anche se al momento tutti i soggetti che trattano i dati per conto della Società come responsabili esterni del trattamento sono stabiliti all'interno dell'Unione Europea, nel futuro potrebbe essere necessario conferire tali dati anche a soggetti che possono essere stabiliti fuori dell'Unione Europea, in paesi che non garantiscono ai dati personali un livello di protezione adeguato ai sensi del Codice Privacy/Regolamento Europeo per la Protezione dei dati RE. EU 679/2016. La società trasferirà, eventualmente, i dati fuori dell'Unione Europea solo previa adozione delle precauzioni stabilite dal Codice Privacy e dal Regolamento Europeo e dopo aver ottenuto dai soggetti indicati le necessarie garanzie e con il consenso degli interessati.

7. Conservazione dei dati

Il Titolare del trattamento conserva e tratta i dati personali per il tempo necessario ad adempiere alle finalità indicate ed in ogni caso per un tempo non superiore a 10 anni, salvo diversi obblighi di legge o la necessità di esercitare diritti, anche in sede giudiziaria da parte della Società.

Quando non è più necessario conservare i dati personali questi verranno cancellati o distrutti

8. Diritti dell'interessato

Ai sensi dell'art. 7 del D. Lgs. 196/2003 e degli articoli dal 15 al 21 del Regolamento, lei potrà esercitare i seguenti diritti:

- il **diritto di accesso** ossia la possibilità di ottenere la conferma che sia o meno in corso un trattamento e di acquisire informazioni in merito a: finalità di esso, categorie di dati personali in questione, destinatari dei dati in particolare se Paesi terzi, il periodo di conservazione ove possibile e le modalità del loro trattamento,
- il **diritto alla rettifica e all'integrazione dei dati**,
- il **diritto alla loro cancellazione**, ogniqualvolta i dati non siano necessari rispetto alle finalità oppure qualora decidesse di revocare il consenso o si opponesse al trattamento o ancora qualora i dati fossero trattati illecitamente;
- il **diritto alla limitazione del trattamento** nel caso in cui contesti l'esattezza dei dati personali per il periodo necessario per effettuare le relative verifiche, oppure il trattamento sia illecito, o qualora benchè il titolare del trattamento non abbia più bisogno dei suoi dati, lei richieda la conservazione per finalità giudiziarie;
- il **diritto alla portabilità dei dati** ad altro titolare, qualora il trattamento avvenga con mezzi automatizzati o sia basato sul consenso;
- il **diritto di opporsi** al trattamento;

Gli stessi, ove da lei esercitabili potranno essere fatti valere scrivendo a infoedatabreach@covar14.it/com specificando l'oggetto della richiesta, il diritto che l'interessato intende esercitare e allegando fotocopia di un documento di identità che attesti la legittimità della richiesta.

8.Proposizione di reclamo

L'interessato ha il diritto di proporre reclamo all'autorità di controllo dello Stato di residenza.

9.Titolare del Trattamento

Il titolare del trattamento è la Società Co.Va.R 14 con sede Carignano (To), Via Cagliero 3I/3L, e potrà contattarla per ogni tematica riguardante i dati personali all'indirizzo sopra riportato o al seguente indirizzo mail infoedatabreach@covar14.it/com

10.Responsabile della protezione

La società Co.Va.R 14 ritenendo di primaria importanza la tutela dei dati personali degli interessati, ha nominato un responsabile della protezione dei dati (DPO) che potrà essere contattato scrivendo all'indirizzo mail dpo@covar14.it/com per ogni tematica riguardante la protezione dei dati personali.

INFORMATIVA SULLA PROTEZIONE DEI DATI

A seguito dell'entrata in vigore del Regolamento europeo n. 16/679 La invitiamo, durante l'attività espletata a favore di Co.Va.R 14 a:

- √ non rendere noto né divulgare o comunicare notizie, informazioni private, conoscenze tecniche relative a nostri utenti/clienti//dipendenti, di cui sia venuto in qualsiasi modo a conoscenza nonché informazioni aziendali inerenti alla proprietà intellettuale;
- √ custodire, controllare e proteggere – in ottemperanza alle disposizioni del Regolamento europeo n. 16/679 – i documenti contenenti dati personali ed eventualmente sensibili riconducibili ai clienti/utenti /dipendenti utilizzati per l'esercizio delle prestazioni;
- √ limitare il salvataggio di dati personali appartenenti a clienti/utenti/dipendenti di Co.Va.R 14 al minimo indispensabile e solo su apparecchi dotati di adeguati dispositivi di protezione;
- √ restituire integralmente a Co.Va.R 14 i dati personali e sensibili in proprio possesso o custodia e che, a seguito della cessazione o modifica delle prestazioni svolte, non si ha più ragione di utilizzare, con espresso divieto di conservarli in copia, duplicarli, comunicarli o diffonderli; quelli memorizzati su supporto elettronico di sua proprietà vanno cancellati in modo definitivo;
- √ segnalare su infoedatabreach@covar14.it e con ogni altro mezzo utile, l'eventuale violazioni di dati personali degli interessati/ dipendenti di Co.Va.R 14 entro le 24 ore dalla scoperta;
- √ presentarsi ai clienti/utenti/dipendenti della società come collaboratori di Co.Va.R 14 senza menzionare e pubblicizzare proprie o altre società di consulenza, salvo diversa ed esplicita autorizzazione;
- √ utilizzare le informazioni inerenti i clienti/utenti/dipendenti di Co.Va.R 14 unicamente per finalità di progetto connesse con lo svolgimento dell'incarico ricevuto, evitando pertanto comunicazioni dirette, comunicando con gli stessi esclusivamente per il tramite della nostra Segreteria;

La informiamo inoltre – ai sensi e per gli effetti dell'art.13 del Codice della privacy e 13 e 14 del Regolamento europeo n. 16/679 – che per il trattamento dei Suoi dati personali di cui è Titolare Co.Va.R 14 le informazioni raccolte presso di Lei, necessarie per eseguire accordi di collaborazione in essere, saranno trattati con mezzi automatizzati o manuali e concernono dati il cui conferimento è facoltativo, ma necessario per lo svolgimento del rapporto. I dati sono conservati sulla base di normativa nazionale ed europea, in particolare per 10 anni dalla cessazione del rapporto d collaborazione.
Il Titolare del trattamento è Co.Va.R 14. Con riferimento agli artt. da 15 a 21 del Reg Eu potrà esercitare i seguenti diritti: di accesso, di rettifica, alla cancellazione, alla limitazione del trattamento, alla portabilità, di opposizione, scrivendo al Titolare del trattamento all'indirizzo sopra riportato, oppure al seguente indirizzo mail infoedatabreach@covar14.it , specificando l'oggetto della sua richiesta, il diritto che intende esercitare e allegando fotocopia di un documento di identità che attesti la legittimità della richiesta oppure può scrivere al DPO designato all'indirizzo dpo@covar14.it
Ogni comunicazione tra le parti avrà luogo esclusivamente per finalità contrattuali e/o misure precontrattuali e per eseguire obblighi di legge nonché per finalità fiscali e contabili.

Letto quanto sopra, La preghiamo di restituirci copia della presente firmata per accettazione.

Data
Firma società

Timbro e firma del professionista per accettazione

_____

INFORMATIVA NUMERO VERDE

Co.va.r.14 in qualità di Titolare del trattamento, intende informarLa, ai sensi dell'articolo 13- 14 Reg. Eu 16/679, in merito al trattamento dei Suoi dati mediante il numero Verde.

1. FINALITÀ DEL TRATTAMENTO

I dati raccolti dal numero verde saranno raccolti per il perseguimento delle seguenti finalità:
- Erogazione di informazioni sul funzionamento della raccolta rifiuti;
- Prenotazione di servizi specifici;
- Segnalazione di disservizi;
- Verifica dei livelli di servizio.

Va evidenziato che, come meglio specificato al punto 5 della presente informativa, Covar14 si avvale per l'attività sopra descritta della Società Pegaso03 S.r.l. nominata per tale ragione responsabile del trattamento ex art. 28 par 2 e 4 Reg. Eu 16/679

2. CONFERIMENTO DEI DATI PERSONALI E BASE GIURIDICA

Il conferimento dei Suoi dati personali è facoltativo, tuttavia l'eventuale rifiuto a fornire i dati strettamente funzionali all'esecuzione dei servizi erogati e/o a renderLe le informazioni su di essi, non comporta alcuna conseguenza in relazione ai rapporti in corso, salva l'eventuale impossibilità di dare seguito alle operazioni connesse a tali dati o l'impossibilità di esecuzione del contratto.

3. MODALITA' DEL TRATTAMENTO

I Suoi dati verranno trattati nel rispetto dei principi di liceità correttezza e trasparenza, utilizzando strumenti manuali o automatizzati anche mediante l'inserimento in banche dati, elenchi e liste idonei alla memorizzazione, gestione e trasmissione dei dati, nei modi e nei limiti necessari al perseguimento delle predette finalità.
La società ha previsto adeguate misure di sicurezza al fine di tutelare i dati personali.
I dati saranno trattati esclusivamente da persone autorizzate al trattamento in relazione alla finalità del trattamento.
I dati non sono oggetto di un processo decisionale automatizzato né di profilazione per le finalità indicate.

4. DESTINATARI DEI DATI

I dati personali trattati dal Titolare non saranno diffusi, ovvero non ne verrà data conoscenza a soggetti indeterminati, in nessuna possibile forma, inclusa quella della loro messa a disposizione o semplice consultazione. Potranno, invece, essere comunicati a Pegaso03 S.r.l., società di erogazione del Servizio di raccolta sul territorio nominati per tale ragione responsabili del trattamento

Ai dati potrebbero accedere (per finalità di assistenza sugli applicativi, sulle reti informatiche e per la connettività) nostri tecnici incaricati o consulenti esterni o incaricati di società che forniscono tali servizi e che per tale ragione sono stati nominati Responsabili del trattamento. Infine, potranno essere comunicati ai soggetti legittimati ad accedervi in forza di disposizioni di legge, regolamenti, normative comunitarie.

5. TRASFERIMENTO DEI DATI

Il Titolare del trattamento non trasferisce i dati personali in Paesi Terzi o a organizzazioni internazionali.

Anche se al momento tutti i soggetti che trattano i dati per conto della Società come responsabili esterni del trattamento sono stabiliti all'interno dell'Unione Europea, nel futuro potrebbe essere necessario conferire tali dati anche a soggetti che possono essere stabiliti fuori dell'Unione Europea, in paesi che non garantiscono ai dati personali un livello di protezione adeguato ai sensi del Codice Privacy/Regolamento Europeo per la Protezione dei dati RE. EU 679/2016. La società trasferirà, eventualmente, i dati fuori dell'Unione Europea solo previa adozione delle precauzioni stabilite dal Codice Privacy e dal Regolamento Europeo e dopo aver ottenuto dai soggetti indicati le necessarie garanzie e con il consenso degli interessati.

6. CONSERVAZIONE DEI DATI

Il Titolare del trattamento conserva e tratta i dati personali per il tempo necessario ad adempiere alle finalità indicate o successivamente trattati ed utilizzando come criterio le norme civilistiche e fiscali italiane in tema di prescrizione.

Quando non è più necessario conservare i dati personali questi verranno cancellati o distrutti.

7. DIRITTI DELL'INTERESSATO

Ai sensi dell'art. 7 del D. Lgs. 196/2003 e degli articoli dal 15 al 21 del Regolamento u 16/679, lei potrà esercitare i seguenti diritti:

- il **diritto di accesso** ossia la possibilità di ottenere la conferma che sia o meno in corso un trattamento e di acquisire informazioni in merito a: finalità di esso, categorie di dati personali in questione, destinatari dei dati in particolare se Paesi terzi, il periodo di conservazione ove possibile e le modalità del loro trattamento,
- il **diritto alla rettifica e all'integrazione dei dati**,
- il **diritto alla loro cancellazione**, ogniqualvolta i dati non siano necessari rispetto alle finalità oppure qualora decidesse di revocare il consenso o si opponesse al trattamento o ancora qualora i dati fossero trattati illecitamente;
- il **diritto alla limitazione del trattamento** nel caso in cui contesti l'esattezza dei dati personali per il periodo necessario per effettuare le relative verifiche, oppure il trattamento sia illecito, o qualora benchè il titolare del trattamento non abbia più bisogno dei suoi dati, lei richieda la conservazione per finalità giudiziarie;
- il **diritto alla portabilità dei dati** ad altro titolare, qualora il trattamento avvenga con mezzi automatizzati o sia basato sul consenso;
- il **diritto di opporsi** al trattamento;

Gli stessi, ove da lei esercitabili potranno essere fatti valere scrivendo a infoedatabreach@covar14.it specificando l'oggetto della richiesta, il diritto che l'interessato intende esercitare e allegando fotocopia di un documento di identità che attesti la legittimità della richiesta.

8. PROPOSIZIONE DEL RECLAMO

L'interessato ha il diritto di proporre reclamo all'Autorità di controllo dello Stato di residenza.

8. TITOLARE DEL TRATTAMENTO

Il titolare del trattamento è il Consorzio Valorizzazione Rifiuti 14, con sede in Carignano, (TO), e potrà contattarlo per ogni tematica riguardante i dati personali all'indirizzo sopra riportato o al seguente indirizzo mailinfoedatabreach@covar14.it

9. RESPONSABILE DELLA PROTEZIONE

Il Covar14 ritenendo di primaria importanza la tutela dei dati personali degli interessati, ha nominato un responsabile della protezione dei dati (DPO) che potrà essere contattato scrivendo all'indirizzo mail dpo@covar14.it per ogni tematica riguardante la protezione dei dati personali.

Informativa sul trattamento dati personali ai sensi dell'art. 13 del D.gvo 196/2003 dell'art. 13 del Regolamento Europeo n. 16/679

Società Co.Va.R 14 (di seguito Consorzio) in qualità di Titolare del trattamento dei dati personali, con sede in Carignano (TO) Via Cagliero 3I/3L/3D, con la presente desidera

INFORMARE

Il/la Sig./ra **……**in seguito definito/a interessato/a, in merito al trattamento dei suoi dati personali in ambito lavorativo.

DATI OGGETTO DEL TRATTAMENTO

I dati che il Consorzio intende trattare sono:

- ✓ Dati anagrafici e/o identificativi;
- ✓ Appartenenza sindacale;
- ✓ Dati relativi alla salute (malattie, infortuni, malattie professionali, invalidità, etc…);
- ✓ Dati di collegamento e/o traffico (indirizzi IP, log degli eventi, etc.);
- ✓ Provvedimenti disciplinari;
- ✓ Vita professionale (curriculum, l'istruzione e la formazione professionale, premi, etc.);
- ✓ Dati personali relativi alle condanne penali e reati;
- ✓ Dati riguardanti i Suoi familiari a carico o componenti del nucleo familiare;
- ✓ Gli estremi del conto corrente bancario.

Tali dati personali, ai sensi dell'art 6 lett b) del Regolamento europeo n. 16/679, possono essere trattati senza il Suo consenso in quanto necessari all'esecuzione del contratto di cui Lei è parte.

Ai sensi dell'art 9 lett. b) del Regolamento europeo n. 16/679, il Consorzio potrà trattare anche **dati personali, cd. particolari,** ossia in grado di rivelare l'originale razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale nonché trattare dati genetici, biometrici, dati relativi alla salute o all'orientamento sessuale, senza il suo consenso, qualora il trattamento sia necessario per assolvere obblighi di legge ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro, nella misura in cui sia autorizzato dal Diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi degli interessati.

1. PRINCIPI APPLICABILI AL TRATTAMENTO DI DATI PERSONALI

Ai sensi dell'art 5 del Regolamento Europeo n. 16/679 I suoi dati sono trattati:

- ✓ in modo **lecito, corretto e trasparente;**

- ✓ in modo **esatto**, e se necessario saranno **aggiornati**;
- ✓ nel rispetto del principio **di pertinenza e non eccedenza** rispetto alle finalità perseguite dal medesimo.

2. FINALITÀ DI TRATTAMENTO

Il trattamento dei Suoi dati personali, forniti in sede di assunzione, è finalizzato unicamente alla gestione del rapporto di lavoro.

In particolare i Suoi dati verranno trattati per:

- ✓ la corretta quantificazione della retribuzione;
- ✓ la gestione del personale;
- ✓ assolvere agli obblighi di legge e di contratto, inclusi quelli derivanti dal contratto collettivo;
- ✓ assolvere agli obblighi nei confronti degli istituti di previdenza ed assistenza, sia obbligatorie che integrative;
- ✓ assolvere agli obblighi nei confronti dell'amministrazione finanziaria;
- ✓ comunicazioni, dietro precise disposizioni di legge o per espressa richiesta dell'interessato, agli enti pubblici territoriali competenti;
- ✓ gestione del contenzioso;
- ✓ gestione e manutenzione del sistema informativo aziendale, compresi i profili della sicurezza;
- ✓ Perseguire l'oggetto del contratto.

Il conferimento dei dati, riguardo alle sopraindicate finalità, è obbligatorio per i dati per cui è previsto un obbligo di legge o in ogni caso necessario all'esecuzione del contratto in oggetto, e l'eventuale rifiuto al trattamento dei suoi dati comporterà l'impossibilità di dare esecuzione al contratto stesso.
La base giuridica del trattamento è l'esecuzione di un contratto

3. MODALITÀ DEL TRATTAMENTO

I suoi dati verranno trattati utilizzando strumenti manuali nonché strumenti informatici anche mediante l'inserimento di essi in banche dati, elenchi e liste idonei alla memorizzazione, gestione e trasmissione dei dati, nei modi e nei limiti necessari al perseguimento delle predette finalità.

Il Consorzio ha previsto adeguate misure di sicurezza al fine di tutelare i Suoi dati personali e aziendali e/o commerciali.

I Suoi dati saranno trattati esclusivamente da persone autorizzate al trattamento all'interno del Consorzio.

Il Consorzio non effettua processi decisionali automatizzati per le finalità sopra descritte.

4. COMUNICAZIONE E TRASFERIMENTO DEI DATI

I suoi dati personali, in considerazione della tipologia contrattuale in essere, possono essere comunicati a Enti che all'uopo possono effettuare operazioni di trattamento dei Suoi dati personali in particolare:

- all'INPS,
- all'INAIL,
- all'Amministrazione Finanziaria,
- a casse e fondi di assistenza e previdenza complementare, in generale ad ogni soggetto pubblico e privato rispetto al quale vi sia per il Consorzio un obbligo o necessità di comunicazione e ciò anche al fine del più corretto adempimento di ogni eventuale obbligo contrattuale;
- alle società di assicurazione;
- alle organizzazioni sindacali;
- alle banche, istituti di credito;

I suoi dati potranno essere anche comunicati a professionisti come consulenti del lavoro, commercialisti, medici del lavoro affinchè trattino i Suoi dati per conto del Consorzio, pertanto, sono stati tutti debitamente nominati Responsabili del trattamento dei dati personali.

Le società informatiche che svolgono attività di manutenzione sui programmi/ piattaforme del Consorzi potrebbero venire a conoscenza dei suoi dati, quindi, anche le suddette società sono state designate Responsabili del trattamento ai sensi dell'art 28 Reg. Eu. 16/679.

In relazione alle proprie mansioni i Suoi dati potranno essere altresì comunicati a fornitori o clienti, Società di formazione ì, compagnie aeree, ferroviarie nonché Hotels per eseguire l'oggetto del contratto.

In caso di necessità i Suoi dati saranno comunicati a Studi legali.

Il Consorzio non trasferisce i Suoi dati personali in Paesi terzi.

5. DIFFUSIONE

I dati personali da Lei messi a disposizione non saranno oggetto di diffusione senza previa autorizzazione.

6. PERIODO DI CONSERVAZIONE DEI DATI PERSONALI

I Suoi dati saranno conservati per tutta la durata del rapporto di lavoro e dalla data di cessazione del predetto rapporto saranno conservati dieci anni per finalità amministrative – contabili salvo obblighi di legge ed esercizio di diritti anche in sede giudiziaria da parte della Società.

7. DIRITTO DEGLI INTERESSATI

Lei, in qualità, di interessato al trattamento dei dati personali potrà esercitare in qualunque momento, i diritti a lei espressamente riconosciuti dal Regolamento europeo, in particolare:

- ✓ **Il diritto di accesso ai dati personali (art. 15)** al fine di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano ed in tal caso, ottenere l'accesso ai dati personali ed alle seguenti informazioni:

- le finalità del trattamento;
- le categorie di dati personali in questione;
- i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
- il diritto di proporre reclamo a un'autorità di controllo;
- qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste da tale trattamento per l'interessato
- dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento dei dati all'estero;

✓ **il diritto di rettifica (art.16)** e di integrazione dei dati personali inesatti o incompleti che la riguardano;

✓ **il diritto alla cancellazione (art. 17)** dei dati personali che la riguardano qualora:

- essi non siano più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati o siano tratti illecitamente oppure ancora debbano essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
- essi siano stati raccolti relativamente all'offerta di servizi delil Covar14dell'informazione di cui all'articolo 8, paragrafo 1;
- revochi il consenso e qualora non sussista altro fondamento giuridico per il trattamento si opponga al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussista alcun motivo legittimo prevalente per procedere al trattamento, oppure si opponga al trattamento ai sensi dell'articolo 21, paragrafo 2;

- **il diritto alla limitazione del trattamento dei dati personali (art. 18)** quando ricorre una delle seguenti ipotesi:
  - Lei contesti l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;

- Il trattamento sia illecito e Lei si opponga alla cancellazione dei dati personali e chieda invece che ne sia limitato l'utilizzo benchè il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria
- Lei si opponga al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto ai propri interessi

- **il diritto alla portabilità dei dati personali** (**art. 20**) ossia di trasmettere tali dati a un altro titolare del trattamento qualora esso si basi sul consenso o su un contratto;
- **diritto di opposizione (art.21)** in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei suoi dati che la riguardano;
- **Il diritto di proporre reclamo ad un'autorità di controllo.**

Qualora ritenesse di esercitare i diritti sopraelencati di seguito viene indicato l'indirizzo mail del Titolare del trattamento a cui potrà rivolgersi a infoedatabreach@covar14.it/com.

8. TITOLARE DEL TRATTAMENTO

Le rammentiamo che il Titolare del trattamento è Co.Va.R 14, con sede in Carignano (To), Via Cagliero 3I/3L/3D. Per ogni questione avente ad oggetto la protezione dei dati personali e/o l'esercizio dei diritti sopra elencati potrà scrivere a infoedatabreach@covar14.it/com.

9. DATA PROTECTION OFFICER

Occorre, in ultimo, informarLa che il Covar14ritenendo di primaria importanza la tutela dei Suoi dati personali, **ha nominato un Data Protection Officer (DPO**) che potrà contattare scrivendo all'indirizzo mail **dpo@covar14.it/com.** per ogni tematica riguardante la protezione dei dati personali.

***

Il/la sottoscritta letta l'informativa:

A seguito della lettura della suddetta informativa La preghiamo di volere restituire all'ufficio personale, la copia della presente da Lei sottoscritta.

Distinti saluti.

Data

_____

Il Covar 14

_____

Timbro + Firma del rapp. legale

Per ricevuta

Sig./ra _____

Informativa sul trattamento dati personali ai sensi dell'art 13 del Regolamento Europeo n. 679/16

CovaR 14 in qualità di Titolare del trattamento dei dati personali, desidera informarla su

1. PRINCIPI APPLICABILI AL TRATTAMENTO DI DATI PERSONALI

ai sensi dell'art 5 del Regolamento Europeo n. 16/679 i Suoi dati saranno trattati in modo:

- ✓ **lecito, corretto e trasparente,**
- ✓ **esatti** ed, in ogni caso se necessario saranno **aggiornati**;
- ✓ pertinente **e non eccedente** rispetto alle finalità perseguite dal medesimo;

2. DATI OGGETTO DEL TRATTAMENTO

i dati che Covar 14 intende trattare sono:

- ✓ Dati anagrafici
- ✓ informazioni su carriera scolastica, situazione professionale, conoscenze specifiche in determinati settori;

3. FINALITÀ DI TRATTAMENTO

I dati da Lei forniti sono trattati per la gestione della procedura concorsuale o selettiva, per l'eventuale conferimento dell'incarico o assunzione, per la gestione delle graduatorie (ove previste nel bando).

In caso di cv ricevuti spontaneamente Le verrà fornita un'adeguata informativa al primo contatto.

4. MODALITÀ DEL TRATTAMENTO

I suoi dati verranno trattati utilizzando strumenti manuali nonché strumenti automatizzati, anche mediante l'inserimento di essi in banche dati, archivi, piattaforme, idonei alla memorizzazione e gestione dei dati, nei modi e nei limiti necessari al perseguimento delle predette finalità.
I Suoi dati saranno trattati esclusivamente da persone autorizzate al trattamento dall'Ente Covar 14.
Sono state previste misure di sicurezza adeguate ai sensi dell'art 32 del Reg. Eu n. 16/679, al fine di prevenire la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. I suoi dati non saranno soggetti a decisioni automatizzate in merito alla finalità sopra indicata.

5. COMUNICAZIONE E TRASFERIMENTO DEI DATI

Le società informatiche che svolgono attività di manutenzione sui programmi/ piattaforme del Covar 14 potrebbero venire a conoscenza dei suoi dati, quindi, le suddette società sono state designate Responsabili del trattamento ai sensi dell'art 28 Reg. Eu. 16/679.
I suoi dati non verranno trasferiti al di fuori dell'Unione Europea.
In caso di necessità i Suoi dati possono essere comunicati a Studi legali.

6. DIFFUSIONE

I dati personali da Lei messi a disposizione non saranno oggetto di diffusione.

7. PERIODO DI CONSERVAZIONE DEI DATI PERSONALI

I Suoi dati saranno conservati per il tempo strettamente necessario al perseguimento delle finalità sopra descritte ed in ogni caso per un tempo non superiore ai 60 gg dalla pubblicazione della graduatoria o dall'atto di pubblicità previsto per i possibili ricorsi, salvo Sua revoca, in ogni momento, del consenso al trattamento dei Suoi dati. In ogni caso i Suoi dati potranno essere trattati per obblighi di legge ed esercizio di diritti anche in sede giudiziaria da parte del Covar 14.

8. DIRITTO DEGLI INTERESSATI

Lei, in qualità, di interessato al trattamento dei dati personali potrà esercitare in qualunque momento, i diritti a lei espressamente riconosciuti dal Regolamento europeo, in particolare:

- ✓ **Il diritto di accesso ai dati personali (art. 15)**: al fine di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano ed in tal caso, ottenere l'accesso ai dati personali ed alle seguenti informazioni:

  - le finalità del trattamento;
  - le categorie di dati personali in questione;
  - i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
  - quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
  - l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
  - il diritto di proporre reclamo a un'autorità di controllo;
  - qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
  - l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste da tale trattamento per l'interessato
  - dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento dei dati all'estero;

- ✓ **il diritto di rettifica (art.16)** e di integrazione dei dati personali inesatti o incompleti che la riguardano;
- ✓ **il diritto alla cancellazione (art. 17)** dei dati personali che la riguardano qualora:

  - essi non siano più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati o siano tratti illecitamente oppure ancora debbano essere cancellati per adempiere un

obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
- revochi il consenso e qualora non sussista altro fondamento giuridico per il trattamento
- si opponga al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussista alcun motivo legittimo prevalente per procedere al trattamento, oppure si opponga al trattamento ai sensi dell'articolo 21, paragrafo 2;

- **il diritto alla limitazione del trattamento dei dati personali (art. 18)** quando ricorre una delle seguenti ipotesi:

  - Lei contesti l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
  - Il trattamento sia illecito e Lei si opponga alla cancellazione dei dati personali e chieda invece che ne sia limitato l'utilizzo
  - i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria benchè il titolare del trattamento non ne abbia più bisogno ai fini del trattamento,
  - Lei si opponga al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto ai Suoi interessi
- **il diritto alla portabilità dei dati personali** (**art. 20**) ossia di trasmettere tali dati a un altro titolare del trattamento qualora esso si basi sul consenso o su un contratto;

- **diritto di opposizione (art.21)** in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei suoi dati che lo riguardano

- **Il diritto di proporre reclamo ad un'autorità di controllo.**

- **Il diritto a revocare il consenso**

Qualora ritenesse di esercitare i diritti sopraelencati di seguito viene indicato l'indirizzo pec del Titolare o all'indirizzo mail infoedatabreach@covar14.it

9. Titolare del Trattamento

Il titolare del trattamento è l'Ente Covar 14 con sede Carignano (TO) in Via Cagliero 3I/3L- e potrà contattarla per ogni tematica riguardante i dati personali all'indirizzo di pec dell'Ente o all'indirizzo mail infoedatabreach@covar14.it

10.Responsabile della protezione

Covar 14 ritenendo di primaria importanza la tutela dei dati personali degli interessati, ha nominato un responsabile della protezione dei dati (DPO) che potrà essere contattato scrivendo all'indirizzo mail dpo@covar14.it per ogni tematica riguardante la protezione dei dati personali.

Preso atto dell'informativa

O Acconsento

O Non acconsento al trattamento dei miei dati personali particolari (dati sanitari, dati che rivelino l'origine razziale o etnica, le opinion politiche, appartenenza a sindacati, condizioni religiose filosofiche)

O Acconsento

O Non acconsento al trattamento dei miei dati anche per annunci di lavoro futuri e diversi da quello per cui ho inviato il cv

DATA E FIRMA

Informativa sul trattamento dati personali ai sensi dell'art 13 del Regolamento Europeo n. 679/16

STAGISTI

Covar 14, in qualità di Titolare del trattamento dei dati personali, con sede in Carignano, Via Cagliero 3I/3L, con la presente desidera

INFORMARE

Il/la Sig./ra _____ in seguito definito/a interessato/a, in merito al trattamento dei suoi dati personali in ambito lavorativo.

In merito allo stage che intende svolgere pressoCovar 14 Co.Va.R. 14 intendiamo informarla su:

1. DATI OGGETTO DEL TRATTAMENTO

I dati cheCovar 14 intende trattare sono:

- ✓ Dati anagrafici;

Ai sensi dell'art 9 lett. b) del Regolamento europeo n. 16/679,Covar 14 potrà trattare anche dati personali, cd. particolari, ossia in grado di rivelare l'originale razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale nonché trattare dati genetici, biometrici, dati relativi alla salute o all'orientamento sessuale, senza il suo consenso, qualora il trattamento sia necessario per assolvere obblighi di legge ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro, nella misura in cui sia autorizzato dal Diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi degli interessati.

2. PRINCIPI APPLICABILI AL TRATTAMENTO DI DATI PERSONALI

Ai sensi dell'art 5 del Regolamento Europeo n. 16/679:

- ✓ I Suoi dati saranno trattati in modo **lecito, corretto e trasparente,**
- ✓ I Suoi dati sono **esatti** ed, in ogni caso se necessario saranno **aggiornati**;
- ✓ Il trattamento dei Suoi dati, rispetta il principio **di pertinenza e non eccedenza** rispetto alle finalità perseguite dal medesimo;
- ✓ è consentito l'accesso ai suoi dati personali solo qualora la conoscenza sia strettamente indispensabile per adempiere ai compiti affidati.

3. FINALITÀ DI TRATTAMENTO

Il trattamento dei Suoi dati personali è finalizzato unicamente a dare esecuzione al rapporto di tirocinio, di formazione ed orientamento, nonché per la gestione del tirocinio, al quale la convenzione sottoscritta in data _____ traCovar 14 Ospitante Co.Va.R. 14 ed il Soggetto Promotore _____del tirocinio, si riferisce.

Il conferimento dei dati, riguardo alle sopraindicate finalità, è facoltativo, tuttavia, il mancato conferimento dei dati determina l'impossibilità di attivare il tirocinio.

4. MODALITÀ DEL TRATTAMENTO

I Suoi dati verranno trattati utilizzando strumenti manuali nonché strumenti automatizzati, anche mediante l'inserimento di essi in banche dati, idonei alla memorizzazione, gestione e trasmissione dei dati, nei modi e nei limiti necessari al perseguimento delle predette finalità.

I Suoi dati saranno trattati esclusivamente da persone autorizzate al trattamento all'interno della Società.

Sono state previste misure di sicurezza adeguate ai sensi dell'art 32 del Reg. Eu n. 16/679, al fine di prevenire la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

La Società non effettua processi decisionali automatizzati per le finalità indicate.

5. COMUNICAZIONE E DIFFUSIONE

I suoi dati potranno essere comunicati a soggetti che hanno necessità di accedere ai Suoi dati per finalità ausiliare al rapporto che intercorre tra Lei eCovar 14 nei limiti strettamente necessari per svolgere tali compiti ausiliari (Ente di formazione che ha promosso il Suo stage, Università presso la quale è iscritto)

I dati personali da Lei messi a disposizione non saranno oggetto di diffusione.

(Oppure) I dati personali da Lei messi a disposizione saranno comunicati a…..per le finalità di…….

6. PERIODO DI CONSERVAZIONE DEI DATI PERSONALI

I Suoi dati saranno conservati per tutta la durata del rapporto di lavoro e dalla data di cessazione del predetto rapporto saranno conservati dieci anni per finalità amministrative – contabili salvo obblighi di legge ed esercizio di diritti anche in sede giudiziaria da parte della Società.

7. DIRITTO DEGLI INTERESSATI

Lei, in qualità, di interessato al trattamento dei dati personali potrà esercitare in qualunque momento, i diritti a lei espressamente riconosciuti dal Regolamento europeo , in particolare:

- ✓ **Il diritto di accesso ai dati personali (art. 15)** al fine di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano ed in tal caso, ottenere l'accesso ai dati personali ed alle seguenti informazioni:
  - le finalità del trattamento;
  - le categorie di dati personali in questione;
  - i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
  - quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
  - l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
  - il diritto di proporre reclamo a un'autorità di controllo;
  - qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
  - l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste da tale trattamento per l'interessato
  - dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento dei dati all'estero;
- ✓ **il diritto di rettifica (art.16)** e di integrazione dei dati personali inesatti o incompleti che la riguardano;
- ✓ **il diritto alla cancellazione (art. 17)** dei dati personali che la riguardano qualora:
  - essi non siano più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati o siano tratti illecitamente oppure ancora debbano essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
  - essi siano stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1;

- revochi il consenso e qualora non sussista altro fondamento giuridico per il trattamento si opponga al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussista alcun motivo legittimo prevalente per procedere al trattamento, oppure si opponga al trattamento ai sensi dell'articolo 21, paragrafo 2;

- **il diritto alla limitazione del trattamento dei dati personali (art. 18)** quando ricorre una delle seguenti ipotesi:
  - Lei contesti l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
  - Il trattamento sia illecito e Lei si opponga alla cancellazione dei dati personali e chieda invece che ne sia limitato l'utilizzo benchè il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria
  - Lei si opponga al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto ai propri interessi
- **il diritto alla portabilità dei dati personali** (**art. 20**) ossia di trasmettere tali dati a un altro titolare del trattamento qualora esso si basi sul consenso o su un contratto;
- **diritto di opposizione (art.21)** in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei suoi dati che la riguardano;
- **Il diritto di proporre reclamo ad un'autorità di controllo.**

Qualora ritenesse di esercitare i diritti sopraelencati o chiedere qualsiasi informazione sul trattamento dei dati di seguito viene indicato l'indirizzo pec del Titolare del trattamento a cui potrà rivolgersi o a infoedatabreach@covar14.it nonché l'indirizzo per posta ordinaria dell'area del personale: coordinamento_pegaso@covar14.it

8. TITOLARE DEL TRATTAMENTO

Le rammentiamo che il titolare del trattamento èCovar 14 Co.Va.R. 14 con sede in Carignano (TO), Via Cagliero 3I/3L.

Per ogni questione avente ad oggetto la protezione dei dati personali e/o l'esercizio dei diritti sopra elencati potrà scrivere a infoedatabreach@covar14.it/com.

9. DATA PROTECTION OFFICER

Occorre, in ultimo, informarLa che Covar 14 ritenendo di primaria importanza la tutela dei Suoi dati personali, **ha nominato un Data Protection Officer (DPO**) che potrà contattare scrivendo all'indirizzo mail dpo@covar14.it per ogni tematica riguardante la protezione dei dati personali.

***

A seguito della lettura della suddetta informativa La preghiamo di volere restituire all'ufficio personale, copia della presente da Lei sottoscritta.

Distinti saluti.

Data

_____

Covar 14 + timbro + firma del rapp legale

Per ricevuta

Sig./ra _____

INFORMATIVA UTENTI

CO.VA.R 14, con sede in Carignano, Via Cagliero n. 3, in qualità di responsabile del trattamento dei dati personali, dei 19 Comuni Consorziati e Titolari del trattamento dei dati, intende renderLe un'adeguata informativa in merito al trattamento dei Suoi dati personali ai sensi dell'art. 13-14 Regolamento europeo sulla protezione dei dati personali n. 16/679 in merito alla gestione unitaria dei rifiuti urbani nella fase di raccolta, avvio recupero e smaltimento.

CATEGORIE DI DATI PERSONALI

I dati personali trattati dall'Ente sono:

- Dati anagrafici;
- Dati contabili;
- Dati particolari;

FINALITÀ DEL TRATTAMENTO

I Suoi dati personali sono trattati per:

- gestione del servizio di elaborazione del Tributo Rifiuti ed emissione dei relativi avvisi di pagamento, comprese le seguenti funzioni:
- predisposizione ed emissione delle bollette;
- valutazione delle richieste degli utenti, a titolo esemplificativo: pagamenti rateizzati, rimborsi, rendicontazione;
- fornire informazioni agli utenti in merito al sistema di tariffazione;
- acquisire domande di variazioni del nucleo familiari
- verificare l'iscrizione degli utenti al servizio ed effettuare le necessarie modifiche es: variazioni, cessazioni nonché verificare le composizioni dei nuclei familiari;
- verificare gli incassi relativi agli avvisi di pagamento e rendicontazione dell'addizionale provinciale;
- gestione degli ecosportelli
- riscossione coattiva del tributo rifiuti

Va evidenziato che, come meglio specificato al punto 5 della presente informativa, Covar 14 si avvale per l'attività sopra descritta della **Società Pegaso 03 srl nominata per tale ragione responsabile del trattamento ex art 28 par 2 e 4 Reg. Eu 16/679**.

I suoi dati personali sono stati ricevuti dal suo Comune di residenza, quale Titolare del trattamento, ed in alcuni casi sono stati comunicati a Pegaso 03 srl, da Lei personalmente o da un Suo delegato.

Il conferimento dei Suoi dati personali è obbligatorio per i soli dati per cui è previsto un obbligo normativo in tal senso. L'Ente, in caso di rifiuto a comunicare tali dati obbligatori, potrà acquisire gli stessi presso terze fonti (ove consentito dalla Legge), ovvero potrà comportare l'impossibilità di renderLe le informazioni ed i servizi richiesti. L'eventuale rifiuto di fornire dati per i quali non sia

previsto un obbligo di conferimento in base alla legge, ma strettamente funzionali all'esecuzione dei contratti in essere o a renderLe le informazioni ed i servizi richiesti, non comporta alcuna conseguenza in relazione ai rapporti in corso, salva l'eventuale impossibilità di dare seguito alle operazioni connesse a tali dati o l'impossibilità di esecuzione del contratto

BASE GIURIDICA

Il trattamento è necessario per adempiere ad un obbligo legale ex art 6 lett. c) Reg. Eu 16/679 nonché ai sensi dell'art 6 lett. e) Reg. Eu 16/679 e dell'art 2-ter del Dlgvo n. 101/2018, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento . Qualora il trattamento di dati particolari non sia necessario per l'esecuzione di un interesse pubblico, i suoi dati saranno trattati solo con il suo consenso che potrà revocare, in ogni momento scrivendo a infoedatabreach@covar14.it.

MODALITÀ DEL TRATTAMENTO

I Suoi dati verranno trattati nel rispetto dei principi di liceità correttezza e trasparenza, utilizzando strumenti manuali o automatizzati anche mediante l'inserimento in banche dati, elenchi e liste idonei alla memorizzazione, gestione e trasmissione dei dati, nei modi e nei limiti necessari al perseguimento delle predette finalità. Sono state previste misure di sicurezza adeguate al fine di tutelare i dati personali. I dati saranno trattati esclusivamente da persone autorizzate al trattamento in relazione alla finalità del trattamento. I dati non sono oggetto di un processo decisionale automatizzato né di profilazione per le finalità indicate.

DESTINATARI DEI DATI

I dati personali trattati dal Titolare non saranno diffusi, ovvero non ne verrà data conoscenza a soggetti indeterminati, in nessuna possibile forma, inclusa quella della loro messa a disposizione o semplice consultazione. Potranno, invece, essere comunicati a Pegaso 03 srl ed ad altre Società dedite all'erogazione del servizio di raccolta rifiuti, con i quali sono stati disciplinati i rapporti privacy

Ai dati potrebbero accedere (per finalità di assistenza sugli applicativi SW, sulle rete informatiche e per la connettività) nostri tecnici incaricati o consulenti esterni o incaricati di società che forniscono tali servizi e che per tale ragione sono stati nominati Responsabili del trattamento. Infine, potranno essere comunicati ai soggetti legittimati ad accedervi in forza di disposizioni di legge, regolamenti, normative comunitarie.

TRASFERIMENTO DEI DATI

I suoi dati non sono trasferiti in Paesi Terzi o a organizzazioni internazionali.

Anche se al momento tutti i soggetti che trattano i dati per conto della Società come responsabili esterni del trattamento sono stabiliti all'interno dell'Unione Europea, nel futuro potrebbe essere necessario conferire tali dati anche a soggetti che possono essere stabiliti fuori dell'Unione Europea, in paesi che non garantiscono ai dati personali un livello di protezione adeguato ai sensi del Codice Privacy/Regolamento Europeo per la Protezione dei dati RE. EU 2016/679. La società trasferirà, eventualmente, i dati fuori dell'Unione Europea solo previa adozione delle precauzioni stabilite dal Codice Privacy e dal Regolamento Europeo e dopo aver ottenuto dai soggetti indicati le necessarie garanzie e con il consenso degli interessati.

CONSERVAZIONE DEI DATI

I dati vengono conservati, secondo quanto prescritto dal Titolare del trattamento, ed in ogni caso, per il tempo necessario ad adempiere alle finalità indicate, secondo quanto previsto dalla legge vigente in materia, salvo la necessità di esercitare diritti anche in sede giudiziaria da parte dell'Ente.

DIRITTI DELL'INTERESSATO

Ai sensi dell'art. 7 del D. Lgs. 196/2003 e degli articoli dal 15 al 21 del Regolamento, lei potrà esercitare i seguenti diritti:

- il **diritto di accesso** ossia la possibilità di ottenere la conferma che sia o meno in corso un trattamento e di acquisire informazioni in merito a: finalità di esso, categorie di dati personali in questione, destinatari dei dati in particolare se Paesi terzi, il periodo di conservazione ove possibile e le modalità del loro trattamento,
- il **diritto alla rettifica** e **all'integrazione dei dati**,
- il **diritto alla loro cancellazione**, ogniqualvolta i dati non siano necessari rispetto alle finalità oppure qualora decidesse di revocare il consenso o si opponesse al trattamento o ancora qualora i dati fossero trattati illecitamente;
- il **diritto alla limitazione del trattamento** nel caso in cui contesti l'esattezza dei dati personali per il periodo necessario per effettuare le relative verifiche, oppure il trattamento sia illecito, o qualora benchè il titolare del trattamento non abbia più bisogno dei suoi dati, lei richieda la conservazione per finalità giudiziarie;
- il **diritto alla portabilità dei dati** ad altro titolare, qualora il trattamento avvenga con mezzi automatizzati o sia basato sul consenso;
- il **diritto di opporsi** al trattamento;

Gli stessi, ove da lei esercitabili potranno essere fatti valere scrivendo a infoedatabreach@covar.it specificando l'oggetto della richiesta, il diritto che l'interessato intende esercitare e allegando fotocopia di un documento di identità che attesti la legittimità della richiesta.

PROPOSIZIONE DI RECLAMO

L'interessato ha il diritto di proporre reclamo all'Autorità di controllo dello Stato di residenza.

TITOLARE E RESPONSABILE DEL TRATTAMENTO

Il titolare del trattamento è il Suo Comune di residenza che potrà contattare agevolmente agli indirizzi messi a disposizione dallo stesso. Covar 14, in qualità di responsabile del trattamento potrà contattarlo per ogni tematica riguardante i dati personali all'indirizzo sopra riportato o al seguente indirizzo mail infoedatabreach@covar14.it

RESPONSABILE DELLA PROTEZIONE

Il COVAR 14 ritenendo di primaria importanza la tutela dei dati personali degli interessati, ha nominato un responsabile della protezione dei dati (DPO) che potrà essere contattato scrivendo all'indirizzo mail dpo@covar14.it per ogni tematica riguardante la protezione dei dati personali.

INFORMATIVA EX ART 13 DEL Reg Eu 16/679 PER VISITATORI

Covar 14 in qualità di titolare del trattamento intende informare i **Visitatori** che è necessario procedere all'identificazione, attraverso l'esibizione di un proprio documento d'identità, dei soggetti esterni che accedono ai locali interni del Covar14 ed alla registrazione del loro nome, cognome, data e ora di entrata, di uscita e, se esistente, della società di appartenenza.

1) **Le finalità del trattamento dei dati personali:** I dati sopra elencati sono registrati per finalità di sicurezza dei locali e delle persone in essi presenti, nonché di controllo e tutela delle informazioni connesse all'attività commerciale delCovar 14.
2) **Natura obbligatoria o facoltativa del trattamento dei dati:** Il conferimento dei dati è facoltativo ma in caso di rifiuto ad esibire il proprio documento d'identità da parte del Visitatore non sarà consentito l'accesso ai locali.
3) **Le modalità di trattamento dei dati personali:** Il trattamento dei dati personali dei Visitatori avviene mediante strumenti informatici, telematici e manuali, con logiche strettamente correlate alle finalità stesse e, comunque, in modo da garantire la sicurezza degli stessi e sempre nel rispetto delle previsioni di cui all'art. 5 del Reg. Eu. 16/679.
4) **Soggetti che possono trattare i dati personali:** I dati dei Visitatori potranno essere trattati dalle persone autorizzate al trattamento, in particolare del servizio reception e da coloro che curano gli aspetti di sicurezza e sorveglianza. I suoi dati non saranno né comunicati a soggetti terzi né diffusi.
5) **Conservazione dei dati:** Il Titolare del trattamento conserva e tratta i dati personali per il tempo necessario ad adempiere alle finalità indicate, in ogni caso per un tempo non superiore a 30 giorni. salvo diversi obblighi di legge e/o la necessità della Società di esercitare diritti anche in sede giudiziale. Successivamente, i dati vengono cancellati.
6) **Diritti dell'Interessato:** La informiamo che il Regolamento europeo all'art. 15 e seg. conferisce all'interessato:

- il **diritto di accesso** ossia la possibilità di ottenere la conferma che sia o meno in corso un trattamento e di acquisire informazioni in merito a: finalità di esso, categorie di dati personali in questione, destinatari dei dati in particolare se Paesi terzi, il periodo di conservazione ove possibile e le modalità del loro trattamento,
- il **diritto alla rettifica e all'integrazione dei dati**,
- il **diritto alla loro cancellazione**, ogniqualvolta i dati non siano necessari rispetto alle finalità oppure qualora decidesse di revocare il consenso o si opponesse al trattamento o ancora qualora i dati fossero trattati illecitamente;
- il **diritto alla limitazione del trattamento** nel caso in cui contesti l'esattezza dei dati personali per il periodo necessario per effettuare le relative verifiche, oppure il trattamento sia illecito, o qualora benchè il titolare del trattamento non abbia più bisogno dei suoi dati, lei richieda la conservazione per finalità giudiziarie;
- il **diritto alla portabilità dei dati** ad altro titolare, qualora il trattamento avvenga con mezzi automatizzati o sia basato sul consenso;
- il **diritto di opporsi** al trattamento;
- **Il diritto a proporre reclamo** avanti all'Autorità.

Qualora decidesse di esercitare i diritti sopra descritti potrà contattare il titolare del trattamento al seguente indirizzo mail infoedatabreach@covar14.it oppure scrivere al titolare del Trattamento

all'indirizzo:pec dell'ente. In ultimo il Covar14 ritenendo di primaria importanza la tutela dei Suoi dati personali, **ha nominato un Data Protection Officer (DPO**) che potrà contattare scrivendo all'indirizzo mail dpo@covar14.it per ogni tematica riguardante la protezione dei dati personali.
Il visitatore, da parte sua non può: scattare foto e effettuare riprese; usare e/o divulgare a terzi le informazioni acquisite nella visita.

INFORMATIVA BREVE

Covar 14 in qualità di titolare del trattamento dei dati personali, con sede in Carignano (TO), Via Cagliero 3I/3L intende informare i visitatori che i dati raccolti all'ingresso della Società sono registrati per finalità di sicurezza dei locali e delle persone in essi presenti e di tutela delle informazioni connesse all'attività della società. I dati vengono conservati per 30 giorni. Il conferimento dei dati è facoltativo ma in caso di rifiuto a comunicarli non potrà avere accesso ai locali. Con riferimento agli artt. 15 e segg. del Reg Eu potrà esercitare i seguenti diritti: di accesso, di rettifica, alla cancellazione, alla limitazione del trattamento, alla portabilità, di opposizione, tali diritti può esercitarli scrivendo al Titolare del trattamento all'indirizzo pec, oppure al seguente indirizzo mail: infoedatabreach@covar14.it, oppure può scrivere al DPO designato all'indirizzo dpo@covar14.it/com. Può proporre reclamo all'Autorità.

Policy Data Breach

e

DPIA

COVAR 14

PREMESSA

Ai fini del presente documento il Titolare del trattamento è identificato con la figura del Rappresentante Legale della società o un Suo delegato in considerazione degli interventi che devono essere decisi in breve tempo.

SCOPO

La presente procedura regolamenta la gestione degli eventi di Data Breach o quelli che vengono, in prima battuta considerati come tali. Si considerano eventi di Data Breach quelli che comportano in modo accidentale o illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trattati da Covar 14 . Tali eventi comportano rischi per i diritti e le libertà degli interessati. I principali rischi sono i seguenti:

- *danni fisici, materiali o immateriali alle persone fisiche,*
- *perdita del controllo dei dati degli interessati*
- *limitazioni dei diritti/discriminazione*
- *furto o usurpazione di identità*
- *perdite finanziarie/danno economico o sociale o reputazionale (sia per l'interessato che per il Rappresentante Legale)*
- *decifratura non autorizzata della pseudonimizzazione*
- *perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari)*

1. GENERALE

1.1 Team crisi

La presente procedura è condivisa con i membri del Team crisi all'atto della loro nomina.

Il team crisi di Covar 14 è composto da:

- DPO nominato
- Data Manager;
- Amministratore di sistema;
- Privacy officer Responsabile Tributo, Area Coordinamento participate,cont. Trib. e .

Possono far parte del team Crisi altri Privacy Officer qualora la violazione dei dati si verificasse nell'area di propria competenza nonché a seconda della verificazione dell'evento Contitolari, responsabili esterni o sub responsabili ove necessario.

Il Team crisi o soggetti da questo delegati, sono i soli autorizzati a trattare con il Garante e con gli interessati.

1.1.1. Formazione del Team crisi

Almeno annualmente il Team crisi effettua una formazione mirata sulla applicazione della presente procedura; tale formazione è effettuata nel caso di introduzione di un nuovo membro nel Team. Nel corso della formazione, si valuta anche la necessità/opportunità di modificare integrare la procedura sulla base

degli eventi eventualmente verificatisi nel corso dell'anno. La formazione e la verifica dell'adeguatezza della procedura debbono essere verbalizzate. Il documento viene archiviato nell'archivio "privacy" di Covar 14 .

1.1.2 Nomina di responsabili esterni, Sub responsabili

Nell'atto della nomina di responsabili esterni, Sub responsabili, deve essere indicato:

- la richiesta di valutazione delle loro procedure di Data Breach;
- la specificazione dei tempi di comunicazione a Covar 14 che deve tener conto delle 72 ore in capo del Rappresentante legale per la segnalazione;
- le conseguenze nel caso di mancata o ritardata comunicazione;
- il riferimento di contatto.

1.1.3 Verbalizzazione delle attività

Tutte le attività e le riunioni del Team crisi debbono essere verbalizzate.

I Verbali sono conservati dal Data Manager, nell'archivio "privacy" di Covar 14 e conservate per almeno 10 anni (o in relazione agli effetti che il Data Breach può avere sui diritti degli interessati). In ogni verbale (sottoscritto dai partecipanti alla riunione) deve essere indicato:

- chi partecipa (membro del Team/invitato all'incontro);
- decisioni assunte nel corso dell'incontro;
- stato di avanzamento delle decisioni assunte nel corso di incontri precedenti.

1.1.4 Disponibilità e Posizione del Rappresentante Legale

Il Rappresentante Legale è tenuto informato degli sviluppi e delle decisioni del Team in ogni fase dell'indagine ed ha potere di imporre misure più restrittive a tutela dei diritti degli interessati. Qualora il Rappresentante Legale non fosse disponibile a fornire il contributo richiesto; il Data Manager ha l'Autorità per procedere autonomamente nelle decisioni prese.

Qualora il Rappresentante Legale non condividesse la decisione presa dal Team e la valutasse eccessiva e tale da impattare negativamente sulla reputazione/immagine della società o ledere gli interessi economici della stessa, si assume la responsabilità di imporre la sua decisione. In questo caso il Team crisi verbalizzerà la decisione del Rappresentante Legale nel MODULO Gestione del Data Breach Sezione S9, la posizione del Team ed archivierà la documentazione senza procedere ulteriormente, tramite comunicazioni con data certa (es. tramite PEC) al Rappresentante Legale.

1.1.5 Ruolo di eventuali esperti esterni

Per le azioni previste dalla procedura possono essere coinvolti eventuali esperti esterni che saranno incaricati previa sottoscrizione di un vincolo di riservatezza.

1.2 Data Breach Policy

Nel sito di Covar 14 è presente la policy di Data Breach ed è posta in modo evidente per favorire, da parte degli interessati la consultazione[1]. La policy è predisposta dall'Organi di Governo di Covar 14 e verificata ad intervalli a cura del Rappresentante Legale/ Data Manager. La finalità della policy è quella di comunicare all'esterno di Covar 14 la presenza di una modalità per la gestione delle segnalazioni che possono portare a situazioni anomale/sospette o Data Breach.
La mail di contatto di segnalazione infoedatabreach@covar14.it è reindirizzata nella casella di posta elettronica delle posizioni organizzative e del personale che coadiuva il data manager indicato espressamente, e dal DPO .
La Data Breach Policy prevede i seguenti contenuti:
Il Covar 14 ha previsto, al fine di tutelare i suoi dati personali, una Data Breach policy, per affrontare al meglio le ipotesi di violazione dei dati personali che coinvolge anche la partecipata Pegaso 03srl in quanto i dati quantitativamente più rilevanti sono quelli inerenti le utenze gestite con designazione di Responsabile/sub-Responsabile alla suddetta società partecipata e perchè, una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, causare danni alla persona fisica.
La violazione dei dati personali può consistere nella distruzione, perdita, modifica, divulgazione non autorizzata o nell'accesso, accidentale od illegale, a dati personali trasmessi, conservati o comunque trattati.

Ai sensi del Regolamento europeo, infatti, i principali rischi per i diritti e le libertà di tutti gli interessati, a seguito dell'avvenuta violazione dei dati sono:

- *danni fisici, materiali o immateriali alle persone fisiche,*
- *perdita del controllo dei dati degli interessati*
- *limitazioni dei diritti/discriminazione*
- *furto o usurpazione di identità*
- *perdite finanziarie/danno economico o sociale o reputazionale (sia per l'interessato che per il Rappresentante Legale)*
- *decifratura non autorizzata della pseudonimizzazione*
- *perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari)*
- *altri…*

Le cause che possono portare a tali situazioni possono essere:

- *errore umano volontario o involontario*
- *circostanze impreviste come incendio, alluvione, terremoto, ecc.*
- *attacco hacker*
- *mancato funzionamento delle misure di mitigazione previste*
- *reati "blagging" in cui le informazioni sono ottenute ingannando l'organizzazione che lo detiene*
- *altre…*

1.3.1. Tempistica

Il calcolo della tempistica (considerando che il GDPR fornisce 72 ore al Rappresentante Legale per la eventuale notifica al Garante e la comunicazione all'interessato) decorre dal ricevimento della segnalazione.

1.4 Rendicontazione delle attività del Team Crisi

[1] Devono essere messe in atto le policy per favorire che l'interessato/Garante/responsabile esterno comunichi tramite la mail infoedatabreach@covar14.it ogni evento; in quanto tale mail è uno dei sistemi di comunicazione costantemente presidiati

Almeno annualmente il Dpo in collaborazione con il Data Manager predispone una relazione sulla attività del Team Crisi nel corso dell'anno. Tale relazione viene trasmessa all'Organo di governo di Covar 14 .

La relazione, per quanto possibile, è integrata da dati numerici per comprendere l'entità degli eventi ed i tempi di reazione.

2. GESTIONE EVENTO DI DATA BREACH

Alla gestione di evento di Data Breach è richiesta la massima attenzione e sensibilità da parte di tutte le funzioni coinvolte.

2.1 Segnalazione

La segnalazione di un evento può provenire:

- Interno – ogni autorizzato al trattamento, nel caso abbia anche il sospetto di una violazione di dati (compiuta dall'interno o dall'esterno) o sia a conoscenza di una comunicazione da parte di un interessato/terzo (anche esterno) deve segnalarlo al proprio Responsabile e quindi ad uno dei membri del Team di crisi in modo da attivare la procedura di valutazione dell'evento; la segnalazione può avvenire con qualsiasi forma, purché sia efficace nel gestire nel minor tempo possibile e ad evidenziare anche un solo sospetto per la valutazione conseguente.
- Esterno (interessato/Garante/stampa) –
    - il Data Manager raccoglie le segnalazioni di possibile Data Breach e le iscrive nella sezione del registro privacy, verifica con il DPO, Team Crisi e i Responsabili coinvolti le modalità di trattamento dell'informazione .
    - il Data Manager comunica via mail con gli altri membri del Team crisi utilizzando la loro casella di posta e quella di infoedatabreach@covar14.it nonché alle comunicazioni telefoniche necessarie.
    - Gestisce la procedura su registro della privacy inserendo tutte le indicazioni previste per tracciare la procedura, consentendo al Dpo di procedere con la relativa segnalazione al Garante nel caso di gestione inerenti i dati di cui sia Titolare Covar 14.
    - Gestisce la procedura su registro della privacy inserendo tutte le indicazioni previste per tracciare la procedura, consentendo al Dpo del Soggetto Titolare del dato di procedere con la relativa segnalazione al Garante nel caso di gestione inerenti i dati di Covar 14 sia solo Responsabile.

2.1.1 ID segnalazione

Ad ogni segnalazione è assegnato un numero univoco (ID) formato dal numero progressivo/anno. Questo numero permetterà di identificare in modo univoco tutta la documentazione che riguarda l'incidente e, per quanto possibile, deve essere sempre indicato.

2.2 Valutazione di pertinenza della segnalazione

Raccolta la segnalazione, attraverso le forme sopra indicate, il Data Manager contatta e convoca, se necessario, nel minor tempo possibile e comunque entro massimo 12 ore dalla segnalazione, tutti i membri ed eventuali altri soggetti potenzialmente coinvolti sulla base delle informazioni disponibili. Qualora qualche membro non fosse disponibile si procede comunque con la riunione.

Il Data Manager compila i campi inerenti la Gestione del Data Breach del programma della Privacy sulla base delle informazioni raccolte e se necessario, anche attraverso il Team e i Responsabili di Area coinvolti, procede nella raccolta di eventuali ulteriori informazioni (es. tramite organi di stampa, richieste di approfondimento) al fine di chiarire la veridicità, la portata e la reale sussistenza dell'evento segnalato.

Il Team crisi valuta le azioni per contenere gli effetti dell'evento, le mette in atto attivando le risorse necessarie e documenta tali azioni nella sezione apposita del programma del Data Breach.

Qualora si verificasse, anche dopo eventuali approfondimenti, la non sussistenza di situazioni che mettono a rischio i dati degli interessati, il Data Manager compila la sezione apposita del programma del Data Breach; comunica gli esiti al Rappresentante Legale (che potrebbe comunque richiedere un ulteriore approfondimento). Il Team valuta la necessità di procedere ad una eventuale Azione correttiva e si procede ad aggiornare il Registro degli incidenti, informando il Rappresentante Legale, rivalutando la conseguenze dell'evento (dati personali colpiti, portata (n. e/o % interessati e n. dati), arco temporale, dati/interessati coinvolti .

Sulla base degli elementi raccolti, valuta la presenza o meno della violazione o presunta tale, tenendo presente che il Team crisi, in caso di dubbio deve assumere un atteggiamento prudenziale a difesa dei diritti dell'interessato e verificare la compilazione delle conseguenti sezioni de registro sia in caso di esito positivo che negativo.

2.3 Analisi del rischio

Il Programma CORA che gestisce il Registro della Privacy è in grado di effettuare una valutazione del rischio in base alla procedura edotta dal documento Enisa "Recommendations for a methodology of the assessment of severity of personal data breaches Working - Document, v1.0, December 2013."

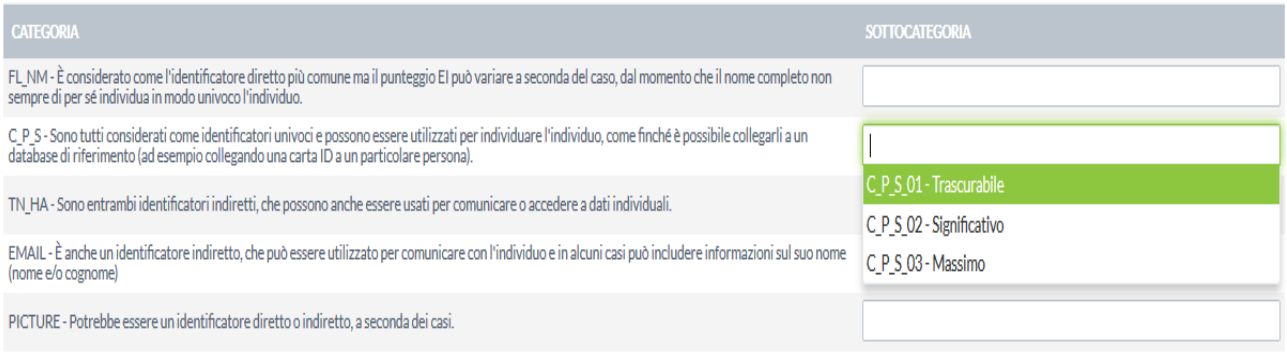
Sull'applicativo, ognuna dei parametro sopraccitato si presenterà come una tabella da implementare in base alle informazioni relative al data breach in esame come di seguito estratto.

- **Sottocategorie dati ai fini del data breach DPC**

NATURA DATI - CATEGORIA	SOTTOCATEGORIA
Dati personali (art. 4 c.1 GDPR) - Dati anagrafici e/o identificativi	
Dati inerente condanne o reati (art. 10 c.1 GDPR) - Dati personali relativi a condanne penali e reati	
Dati particolari (art. 9 c.1 GDPR) - Dati inerenti l'appartenenza al sindacato	Dati inerenti l'appartenenza al sindacato (1) - Dati di appartenenza sindacale di esponenti che rivestono incarichi pubblici Dati inerenti l'appartenenza al sindacato (2) - Dati di appartenenza sindacale deducibili dal contesto (eventi, manifestazioni, etc..) Dati inerenti l'appartenenza al sindacato (3) - Dati di appartenenza sindacale dedotti da fonti sindacali (tesseramenti, congressi, etc..) Dati inerenti l'appartenenza al sindacato (4) - Dati di appartenenza sindacale dedotti da gruppi social segreti o aree internet ad accesso selezionato (intranet)
Dati particolari (art. 9 c.1 GDPR) - Dati inerenti le convinzioni religiose e/o filosofiche	
Dati particolari (art. 9 c.1 GDPR) - Dati Biometrici	
Dati particolari (art. 9 c.1 GDPR) - Dati Genetici	
Dati particolari (art. 9 c.1 GDPR) - Dati inerenti l'origine etnica e razziale	
Dati particolari (art. 9 c.1 GDPR) - Dati inerenti la salute (malattie, infortuni, malattie professionali, invalidità, appartenenza a categorie protette, etc...)	

In questa sezione sarà necessario andare a selezionare le categorie dei dati oggetto del data breach.

- **Facilità di Individuazione (EI)**



I valori di tale sezione sono da selezionare in base ai seguenti criteri:

- **FL_NM (Full name)**
  - **FL_NM_01 - Trascurabile:** in relazione a tutta la popolazione di un paese dove molte persone condividono lo stesso nome e cognome;
  - **FL_NM_02 - Limitato:** in relazione a tutta la popolazione di un paese dove poche persone condividono lo stesso nome e cognome;
  - **FL_NM_03 - Significativo:** in relazione alla popolazione di una piccola città in cui poche o nessuna persona lo condivide;
  - **FL_NM_04 - Massimo:** in relazione alla popolazione di un paese in al nome vengono associati data di nascita e e-mail.

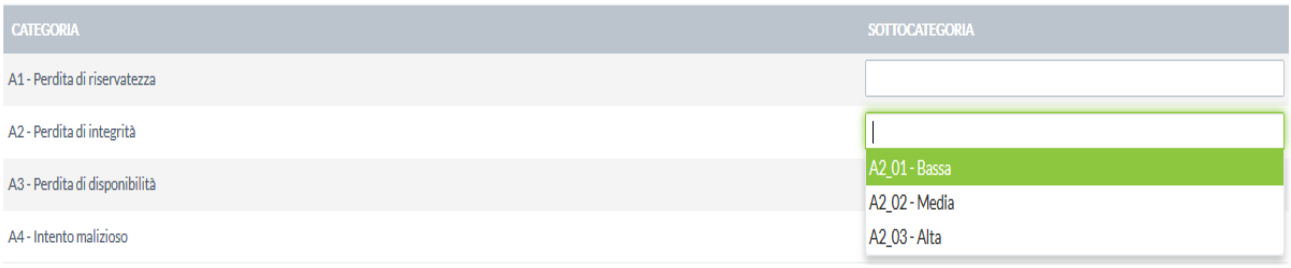
- **C_P_S (ID / passport / social security number)**
  - **C_P_S_01 - Trascurabile:** quando non sono fornite altre informazioni sull'individuo o non sia possibile conoscerle a meno che non si abbia accesso al database di riferimento;
  - **C_P_S_02 - Significativo:** quando l'identificatore rivela ulteriori informazioni di identificazione sull'individuo (ad esempio numero di previdenza sociale che rivela la data di nascita) ed è collegato ad altri dati (ad es. indirizzo postale o email).
  - **C_P_S_01 - Massimo:** quando sono disponibili anche le informazioni dal database di riferimento (ad esempio carta d'identità e nome completo e / o immagine).

- **TN_HA (Telephone number / Home address)**
  - **TN_HA_01 - Trascurabile:** nella popolazione di un paese quando il numero / indirizzo non è registrato in un registro disponibile al pubblico.
  - **TN_HA_02 - Significativo:** nella popolazione di una piccola città e il numero / indirizzo non è registrato in un registro accessibile al pubblico (identificazione possibile tramite comunicazione).
  - **TN_HA_01 - Massimo:** nella popolazione di un paese e il numero / indirizzo è incluso in registro pubblico.

- **PICTURE (picture)**
  - **PICTURE_01 - Trascurabile:** quando l'immagine non è chiara o vaga
  - **PICTURE_02 - Limitato:** quando l'immagine non è chiara o vaga ma include informazioni aggiuntive (ad esempio dintorni che mostrano una posizione specifica) che potrebbero portare all'identificazione.
  - **PICTURE_03 - Significativo:** quando l'immagine è chiara ma non ci sono altre informazioni di identificazione collegate ad essa.
  - **PICTURE_04 - Massimo:** quando l'immagine è chiara e collegata ad alcune informazioni aggiuntive (ad es. informazioni sull'appartenenza a un gruppo specifico, indirizzo di casa, ecc.).

- **C_A_I (Coding / Aliases / Initials)**
  - **C_A_I_01 - Trascurabile:** quando il codice / alias non rivela e non può essere collegato a nessun altro dati personali sulla persona a meno che non si abbia accesso al database di riferimento.
  - **C_A_I_02 - Significativo:** quando l'alias rivela alcuni dati sull'individuo (ad es. Nome) ed è collegato ad altri dati personali (ad esempio l'indirizzo email dell'individuo).
  - **C_A_I_01 - Massimo:** quando l'alias rivela il nome completo dell'individuo o i dati dal database di riferimento sono disponibili.

- **Contesto della violazione (CB)**



I valori di tale sezione sono da selezionare in base ai seguenti criteri:

- **A1 - Perdita di riservatezza**
  - **A1_01 - Bassa (Peso 0)**
    - Esempi di dati esposti a rischi di riservatezza senza prove di trattamento illegale:
      - Un file cartaceo o un laptop si perde durante il transito.
      - L'attrezzatura è stata smaltita senza distruzione dei dati personali
  - **A1_02 - Media (Peso 0,25)**
    - Esempi di dati disposti per un certo numero di destinatari noti:
      - Un'e-mail con dati personali è stata inviata erroneamente a un certo numero di destinatari noti.

- Alcuni clienti possono accedere agli account di altri clienti in un servizio online.

- **A1_03 - Alta (Peso 0,5)**
  - Esempi di dati disposti a un numero sconosciuto di destinatari:
    - I dati sono pubblicati su una bacheca internet;
    - I dati sono caricati su un sito P2P.
    - Un dipendente vende un CD ROM con i dati del cliente.
    - Un sito Web configurato in modo errato rende accessibili pubblicamente i dati Internet dall'interno utenti.

- **A2 - Perdita di integrità**
  - **A2_01 - Bassa (Peso 0)**
    - Esempi di dati modificati ma senza alcun uso errato o illegale identificato:
      - I registri di un database con dati personali sono stati aggiornati erroneamente ma l'originale è stato ottenuto prima che si verifichi qualsiasi utilizzo dei dati modificati.
  - **A2_02 - Media (Peso 0,25)**
    - Esempi di dati modificati ed eventualmente usati in modo errato o illegale ma con possibilità di riprendersi:
      - È stato modificato un record necessario per la fornitura di un servizio sociale online e l'individuo ha bisogno di chiedere il servizio in modo offline.
      - Un record importante per l'accuratezza del file di un individuo in un medico online è stato modificato.

  - **A2_03 - Alta (Peso 0,5)**
    - Esempi di dati modificati ed eventualmente usati in modo scorretto o illegale senza possibilità di recuperare:
      - Gli esempi precedenti se l'originale non può essere recuperato.

- **A3 - Perdita di disponibilità**
  - **A3_01 - Bassa (Peso 0)**
    - Esempi di dati che possono essere recuperati senza difficoltà:
      - Una copia del file è persa ma sono disponibili altre copie
      - Un database è danneggiato ma può essere facilmente ricostruito da altri database.
  - **A3_02 - Media (Peso 0,25)**
    - Esempi di indisponibilità temporale:
      - Un database è danneggiato ma può essere ricostruito da altri database, anche se alcuni caso è richiesta un'elaborazione.
      - Un file è andato perso ma le informazioni possono essere fornite di nuovo dall'individuo.
  - **A3_03 - Alta (Peso 0,5)**
    - Esempi di indisponibilità totale (i dati non possono essere recuperati dal controller o da altri individui):
      - Un file è andato perso / il database è danneggiato, non c'è il backup di questa informazione, e non può essere fornita dall'individuo.

- **A4 - Intento malevolo**
  - **A4_01 - Alta (Peso 0,5)**
    - Se la violazione è dovuta a un'azione intenzionale, ad es. per causare problemi ai dati al titolare dei dati e / o al fine di danneggiare le persone.
      - Un dipendente di un'azienda condivide intenzionalmente dati privati di clienti in un contesto pubblico multimediale (social network)
      - Un dipendente di un'azienda vende dati privati dai clienti a un'altra società.
      - Un membro di un social network invia intenzionalmente informazioni sugli altri membri ai propri familiari per danneggiarli.

Dopo aver analizzato attentamente e definito le risposte per tali criteri, premendo il pulsante 

, verrà restituito il calcolo della gravità del data breach in base alla formula sopraccitata:

2.4 Comunicazione al Garante ed agli interessati

A seguito di un evento di DataBreach che riguardi i dati di cui Covar è titolare, deve essere effettuata la comunicazione al Garante ed agli interessati. La comunicazione è coordinata dal Team Crisi. Le evidenze di tutte le comunicazioni debbono essere conservate.

2.4.1 Comunicazioni al Garante

La comunicazione al Garante deve contenere almeno i seguenti elementi:

- Riferimenti della azienda e del Rappresentante Legale
- Indirizzo PEC e/o EMAIL per eventuali comunicazioni
- Recapito telefonico per eventuali comunicazioni
- Eventuali Contatti (altre informazioni)
- Natura della comunicazione
- Breve descrizione della violazione dei dati personali trattati
- Quando si è verificata la violazione dei dati personali trattati Specificare arco temporale o se la violazione è ancora in corso
- Dove è avvenuta la violazione dei dati? (es. se avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)
- Tipo di violazione
- Lettura (presumibilmente i dati non sono stati copiati)
- Copia (i dati sono ancora presenti sui sistemi del Rappresenta Legale)
- Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- Cancellazione (i dati non sono più sui sistemi del Rappresenta Legale e non li ha neppure l'autore della violazione)

- Furto (i dati non sono più sui sistemi del Rappresenta Legale e li ha l'autore della violazione)
- Dispositivo oggetto della violazione ed eventuale ubicazione (es. Computer, Rete, Dispositivo mobile, Archivio/File o parte di un archivio/file, Strumento di *backup,* Documento cartaceo)
  Altro:
- Quanti interessati sono state colpiti dalla violazione dei dati personali N. interessati ed incidenza % sull'universo della popolazione/ Un numero (ancora) sconosciuto di interessati
- Che tipo di dati sono oggetto di violazione
- Misure tecniche e organizzative applicate ai dati oggetto di violazione
- Eventuali azioni già intraprese per contenere la violazione
- Eventuali azioni già intraprese per ripristinare lo status quo (quando possibile)
- Eventuali azioni correttive
- La violazione è stata comunicata anche agli interessati?
- Sì, è stata comunicata il …e mezzo utilizzato
- No, perché
- Allegare l'analisi del rischio estrapolata dal MODULO Gestione del Data Breach e l'eventuale comunicazione inviata agli interessati

2.4.2 Comunicazione agli interessati

La comunicazione agli interessati può avvenire con modalità diverse tra cui:

- comunicazione diretta agli interessati
- comunicato stampa
- comunicazione tramite sito WEB/social media
- altre forme

La comunicazione deve essere congruente con quanto indicato nella data Breach Policy.

Il Data Manager ha la responsabilità per:

- individuare la/le forma/e di comunicazione da utilizzare
- la responsabilità per la stesura ed approvazione delle comunicazioni
- il livello di coinvolgimento del Team crisi nella comunicazione verso l'esterno; in ogni caso il Team crisi non può essere escluso

Il Team crisi decide la strategia di *crisis communication* da mettere in atto da quando è a conoscenza dell'evento di Data Breach ed anche successivamente quando l'evento è stato risolto.

Di seguito le linee guida da considerare per la redazione delle comunicazioni verso gli interessati

Aspetti generali:

- definire il tono della comunicazione che può essere più informare (comunicato) o più formale (dichiarazione ufficiale)
- fornire un titolo "giornalistico" che per quanto possibile rassicuri gli interessati o perlomeno riducano il livello di allarme, utilizzare parole chiave facilmente rintracciabili sui motori di ricerca qualora venissero ricercate informazioni sui motori di ricerca
- le comunicazioni potrebbero non riguardare solo il Data Breach (rilevazione) ma anche le informazioni sull'andamento dello stesso nel tempo
- assicurare forme di comunicazione oneste, concrete e trasparenti

- fare riferimento al Team crisi, il suo ruolo ed il suo impegno
- mettere in evidenza la storia, l'impegno della azienda nell'assicurare l'attenzione al tema, gli investimenti fatti, le misure applicate
- descrivere l'evento in modo facilmente comprensibile, quale impatto ha avuto sui dati (o quale impatto presumibile può avere – informazioni perse, violate, comunicate a terzi non autorizzati, diffuse, ecc), come lo si sta affrontando/è stato affrontato, specificare cosa l'azienda sta facendo concretamente per proteggere i dati degli interessati
- indicare come e quando è stato coinvolto il Garante della Protezione dei dati
- inserire un contatto diretto per contattare l'organizzazione
- considerare l'utilizzo del numero verde per rispondere agli interessati

Aspetti specifici per il comunicato stampa/dichiarazione ufficiale:

- prevedere link a pagina del sito web dove sono reperibili ulteriori informazioni sul Data Breach ed anche lo stato dell'andamento dello stesso nel tempo

Aspetti specifici per la comunicazione tramite sito WEB/social media:

- considerare di pubblicare (per le situazioni più gravi) anche un video di scuse/spiegazioni coinvolgendo il top management, affidarsi ad un esperto, qualora non si disponesse internamente di tali competenze, per evitare errori o creare più allarme del necessario
- considerare di attivare una APP dedicata all'evento

La comunicazione agli interessati deve contenere almeno i seguenti elementi:

Mittente:
Destinatario: [Nome e indirizzo dell'interessato colpito], data [gg/mm/aaa di riscontro della violazione dei dati personali,
Conseguenze delle violazioni, i dati personali potrebbero essere stati:

- Divulgati
- Distrutti
- Persi
- Modificati
- È stato eseguito l'accesso
- Altro [specificare]

da persone non autorizzate.
misure da implementare, indirizzi per contattare in Covar 14 via mail (infoedatabreach@covar14.it) o via posta all'indirizzo pec

2.8 Comunicazione all'Organo di governo di Covar 14 .

A seguito di un evento che ricade nei casi di data breach, deve essere tenuto aggiornato da parte del DPO il Legale Rappresentante dell'Ente con comunicazioni rintracciabili.

2.9 Situazioni anomale o di emergenza

In caso di segnalazioni in situazioni anomale o di emergenza, quali:

- chiusura temporanea della sede di Covar 14 (es. periodo di ferie)
- mancanza di figure apicali del Team crisi
- mancanza di collegamenti (es. internet)/energia/situazioni di emergenza dovute a cause di forza maggiore)

Devono essere considerate le seguenti misure:

- Il Team crisi può operare anche con una sola persona tra quelle che compongono il Team

Le riunioni del Team possono essere effettuate in luoghi diversi dalla sede di Covar 14 e via telefono o via mail.

3. DPIA- VALUTAZIONE

Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, chiede un parere al responsabile della protezione dei dati
Qualora all'esito di tale valutazione il titolare ritenga che il trattamento presentI un rischio elevato per i diritti e le libertà delle persone fisiche coinvolte, dovrà consultare l'Autorità di controllo, secondo quanto disposto dall'art. 36 del Regolamento (consultazione preventiva).
La valutazione d'impatto sulla protezione dei dati è richiesta in particolare nei seguenti casi:

- una valutazione sistematica e globale di aspetti della personalità degli interessati, basata sulla profilazione e da cui discendono decisioni che hanno effetti giuridici sugli interessati o incidono gravemente sugli interessati;
- il trattamento su larga scala di categorie particolari di dati personali, dati biometrici o dati relativi a condanne penali e reati o a connesse misure di sicurezza;
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

La valutazione è obbligatoria in determinati casi, come nell'ipotesi in cui si debba procedere al trattamento di dati:

- biometrici;
- relativi a condanne penali e reati o a connesse misure di sicurezza.

La valutazione è effettuata in relazione ai seguenti parametri:

- Riservatezza: stima del danno/impatto che la perdita di riservatezza riguardante l'asset comporterebbe per il business di Covar 14 /tutela interessato
- Integrità: stima del danno/impatto che la perdita di integrità riguardante l'asset comporterebbe per il business di Covar 14 /tutela interessato
- Disponibilità: stima del danno/impatto che la perdita di disponibilità riguardante l'asset comporterebbe per il business di Covar 14 /tutela interessato

4. Tabella dei parametri di impatto

Per la valutazione della stima della perdita di Riservatezza, Integrità e Disponibilità viene utilizzata la seguente tabella.

La tabella dei parametri di impatto sui trattamenti permette di definire come alcuni parametri influiscono (impattano) sul rischio di un trattamento.
Tutti i parametri che si mettono all'interno di una stessa classe sono mutuamente esclusivi all'interno della classe quando sono utilizzati in fase di valutazione di impatto. di default sul sistema ci sono i seguenti valori:

CLASSE DI IMPATTO	DESCRIZIONE	IMPATTO SU RISERVATEZZA	IMPATTO SU INTEGRITA'	IMPATTO SU DISPONIBLITA'
VOLUME DI DATI	Trattamento con meno di 5000 informazioni registrate	Basso	N/A	Basso
VOLUME DI DATI	Trattamento con un numero di informazioni registrate tra 5000 e 1.000.000	Medio / Alto	N/A	Medio / Basso
VOLUME DI DATI	Trattamento con un numero di informazioni registrate superiore a 1.000.000	Alto	N/A	Medio / Alto
PROFILAZIONE	Trattamento che non opera profilazione	Basso	Basso	N/A
PROFILAZIONE	Trattamento che opera profilazione	Medio / Alto	Medio / Basso	N/A
SORVEGLIANZA	Trattamento che non opera sorveglianza su larga scala in spazi aperti al pubblico	Bassa	N/A	N/A
SORVEGLIANZA	Trattamento che opera sorveglianza su larga scala in spazi aperti al pubblico	Medio / Alto	N/A	N/A
RISERVATEZZA	I dati sono pubblici	Basso	N/A	N/A
RISERVATEZZA	I dati NON sono pubblici ma comunque NON sono soggetti a particolari vincoli di riservatezza	Basso	N/A	N/A

RISERVATEZZA	I dati sono riservati per finalità di business; una eventuale loro indebita diffusione potrebbe comportare conseguenze importanti sul business o violazioni di legge	Medio / Basso	N/A	N/A
RISERVATEZZA	I dati sono riservati per finalità di business; una eventuale loro indebita diffusione potrebbe comportare conseguenze (concorrenza sleale, danni all'immagine, etc..) elevate sul business	Medio / Alto	N/A	N/A
RISERVATEZZA	La diffusione indebita dei dati trattati è così grave che può mettere a repentaglio la sussistenza dell'organizzazione	Alto	N/A	N/A
INTEGRITA'	I dati non hanno particolari requisiti di integrità	N/A	Basso	N/A
INTEGRITA'	I dati non fanno parte e non influenzano transazioni economiche, finanziarie, sanitarie o di profilazione	N/A	Basso	N/A
INTEGRITA'	I dati trattati fanno parte o influenzano transazioni	N/A	Medio / Basso	N/A

	economiche, finanziarie con impatti sul business. La mancanza di integrità dei dati ha elevati impatti sulle attività operative, ma non sul rispetto delle normative vigenti.			
INTEGRITA'	I dati trattati fanno parte o influenzano transazioni economiche, finanziarie con impatti sul business. La mancanza di integrità dei dati ha anche impatti sulle attività operative e sul rispetto delle normative vigenti.	N/A	Medio / Alto	N/A
INTEGRITA'	I dati trattati fanno parte o influenzano transazioni economiche, finanziarie, sanitarie o di profilazione. La mancanza di integrità dei dati ha elevati impatti sulle attività operative e sul rispetto delle normative vigenti.	N/A	Alto	N/A
DISPONIBILITA'	Per i dati trattati non sono stabiliti a livello contrattuale o normativo tempi massimi di indisponibilità	N/A	N/A	Basso
DISPONIBILITA'	Sono stabiliti, a livello contrattuale o normativo, tempi massimi di	N/A	N/A	Basso

	indisponibilità. Tuttavia il superamento dei tempi stabiliti comporta violazioni contrattuali, multe o penali irrilevanti.			
DISPONIBILITA'	Sono stabiliti, a livello contrattuale o normativo, tempi massimi di indisponibilità. Il superamento dei tempi stabiliti comporta violazioni contrattuali, multe o penali non particolarmente rilevanti.	N/A	N/A	Medio / Basso
DISPONIBILITA'	Sono stabiliti, a livello contrattuale o normativo, tempi massimi di indisponibilità. Il superamento dei tempi stabiliti comporta violazioni contrattuali, multe o penali rilevanti.	N/A	N/A	Medio / Alto
DISPONIBILITA'	Sono stabiliti, a livello contrattuale o normativo, tempi massimi di indisponibilità. Il superamento dei tempi stabiliti comporta violazioni contrattuali, multe o penali che mettono in pericolo la sostenibilità economica e di immagine.	N/A	N/A	

3.2 Dati violati oggetto di DPIA - Criteri di valutazione ed esoneri DPIA

In linea con il Programa di gestione della privacy si ribadisce che le Linee-guida concernenti valutazione impatto sulla protezione dati (WP 248) del gruppo di lavoro art. 29 WP contengono importanti informazioni concernenti la DPIA, in particolar modo un elenco di casi in cui è necessario effettuare una valutazione d'impatto e di casistiche di esonero.

Dopo aver terminato il questionario di Privacy by Design e by Default (con esito positivo), il software porterà ad una nuova scheda: "Criteri di Valutazione DPIA" contenente due voci:

- CASISTICHE DPIA
- ESONERI DPIA

Da questi elenchi si riterrà necessario indicare se il trattamento che stiamo costruendo rientra in una o più di quelle casistiche.

attenzione Se durante la definizione delle casistiche DPIA sono stati definiti dei parametri di uscita per la preselezione, nella scheda di "Criteri di Valutazione DPIA" nel sottomenù CASISTICHE DPIA, è possibile che alcune di queste casistiche siano preselezionate. Se preselezionate, sotto il campo "PRESELEZIONATO IN QUESTIONARIO" comparirà un segno per indicare la scelta definita nel questionario. Nell'esempio qui sotto, vediamo che non era stata preselezionata alcuna casistica.

PRESELEZIONATO IN QUESTIONARIO	NOME	DESCRIZIONE
☑	Nessuna casistica DPIA	Nessuna casistica DPIA
☐	Combinazione o raffronto di insiemi di dati	Combinazione o raffronto di insiemi di dati, per esempio derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato
☐	Dati relativi a interessati vulnerabili	Il trattamento di questa tipologia di informazioni rappresenta un criterio ai fini della DPIA in quanto è più accentuato lo squilibrio di poteri fra interessato e titolare del trattamento, nel senso che il singolo può non disporre del potere di acconsentire, o di opporsi, con facilità al trattamento dei propri dati, né può talora con facilità esercitare i propri diritti. La categoria degli interessati vulnerabili comprende anche i minori, che, si può ritenere non siano in grado di opporsi o acconsentire, in modo consapevole e ragionato, al trattamento dei propri dati personali, i dipendenti, quei segmenti di popolazione particolarmente vulnerabile e meritevole di specifica tutela (soggetti con patologie psichiatriche, richiedenti asilo, anziani, pazienti) e ogni interessato per il quale si possa identificare una situazione di disequilibrio nel rapporto con il rispettivo titolare del trattamento.

Dopo aver scelto le voci più opportune, verrà restituito un esito che potrà essere:

- DPIA: Se la somma delle casistiche di rischio in cui ricade il trattamento ha peso >= a 2 e non ha alcun esonero, il sistema ci consiglierà di effettuare la Valutazione d'Impatto.
- NO DPIA: Se la somma delle casistiche di rischio in cui ricade il trattamento ha peso < 2 o se ha almeno un esonero, il sistema ci informerà che non sarà necessario effettuare una DPIA.

attenzione E' importante notare che, qualsiasi sia l'esito restituito dal software, ci verrà richiesto di assumere la decisione definitiva circa la necessità di effettuare la DPIA.

Di default l'esito temporaneo sarà 

.

- Selezionando 

, lo stato rimarrà su WAIT. Sarà possibile salvare le modifiche premendo il pulsante conferma e riprendere la valutazione in un secondo momento.
- Selezionando 

, l'esito diverrà "NO DPIA" ma occorrerà indicare le motivazioni per tale scelta e l'anagrafica che ha approvato tale valutazione.
- Selezionando 

, l'esito diverrà "DPIA" e, anche in questo caso, occorrerà indicare le motivazioni per tale scelta e l'anagrafica che ha approvato tale valutazione.

Esempio di motivazione: "Il Titolare tramite i soggetti da lui preposti, sentito anche il parere del Responsabile della protezione dei dati ai sensi dell'art. 39 paragrafo 1 lettera c del Regolamento Europeo 2016/679, conclude ed approva la seguente valutazione di impatto, condotta ai sensi dell'art. 35 del Regolamento Europeo 2016/679, quale strumento atto a presidiare i rischi per i diritti e le libertà delle persone fisiche oggetto di trattamento."

Una volta definita la propria scelta, possiamo CONSOLIDARE LA VALUTAZIONE selezionando il campo 

e premendo successivamente il pulsante 

.

attenzione Una volta consolidato la valutazione e premuto il pulsante "CONSOLIDA VALUTAZIONE, **non sarà più possibile modificare le casistiche, gli esoneri e il resto dei dati riguardante la valutazione**. Se l'esito è "DPIA", si aprirà automaticamente un popup contenente il questionario DPIA. Se l'esito è "NO DPIA", si verrà automaticamente indirizzati alla scheda di aggiunta di un nuovo trattamento, dove alcuni campi saranno già valorizzati con i valori indicati precedentemente.

Possiamo ora proseguire con il questionario dedicato alla DPIA.

In ogni caso, qualora il trattamento oggetto della violazione non fosse stato sottoposto ad una DPIA, ma nel corso dell'analisi emergesse un'errata valutazione sulle ragioni che avevano determinato l'omessa valutazione d'impatto del rischio ex art 35 GDPR o qualora si prendesse semplicemente atto della mancanza di una DPIA nel calcolo del rischio si ritiene di applicare la posizione più prudenziale, quindi, risulta necessario associare al trattamento oggetto della valutazione, il punteggio massimo (valore 6).

2.4 Esito della analisi del rischio e decisioni

Il questionario è così composto:

- **I SETTE PRINCIPI:** I principi della Privacy by Design analizzati;
- **PARERI**: In questa sezione è possibile indicare i pareri degli interessati ed eventuali altri soggetti a supporto dell'iniziativa;

- **I CRITERI D'IMPATTO**: Analisi degli impatti ai fini di stabilire l'importanza dei dati trattati. (tra cui l'analisi su Riservatezza, Integrità, Disponibilità, volume dei dati, profilazione, ecc...). Possono essere gestiti secondo le istruzioni

Terminata la prima parte riguardante i sette principi e i criteri di impatto, si entra nell'ultima parte dedicata alla verosimiglianza minacce e alle misure di sicurezza.

- **VEROSIMIGLIANZA MINACCE**: Indicazione della probabilità (o verosimiglianza) dell'accadimento di una determinata minaccia;
- **MISURE DI SICUREZZA**: Indicazione delle misure di sicurezza implementate per contrastare i rischi.
- **SINTESI DEL RISCHIO**: Propone il calcolo dell'impatto dei rischi e l'efficacia delle relativa misure di sicurezza indicate precedentemente;

Questa sezione non è altro che la PRA (Privacy Risk Assessment). La PRA viene condotta sia sulle iniziative che sul trattamenti in essere poichè fa parte di quei controlli riguardanti minacce e misure di sicurezza che occorre riproporre ciclicamente sui trattamenti.

Al termine della PRA si aprirà la scheda "Sintesi del Rischio" che presenterà un prospetto indicante la percentuale di rischio lordo e rischio netto definito per ogni minaccia indicata nella scheda "Verosimiglianza minacce" dove:

- Per RISCHIO LORDO si intende il rischio che incombe un un trattamento;
- Per RISCHIO NETTO si intende il rischio residuo dopo l'applicazione delle misure di sicurezza definite nella scheda "Misure di sicurezza".

CLASSE	CATEGORIA	MINACCIA	RISCHIO LORDO O INERENTE	RISCHIO NETTO/RESIDUO	DETTAGLI
Compliance normativa	Compliance	Raccolta eccessiva di dati personali	9,6	6,92	DETTAGLI
		Accesso non autorizzato ai dati personali	3,2	2,64	DETTAGLI
		Informazioni insufficienti sulle finalità ai soggetti interessati	6,4	2,64	DETTAGLI
		Diritti dell'interessato non rispettati	12,8	7,56	DETTAGLI
		Trattamento non autorizzato di dati personal	6,4	3,24	DETTAGLI
		Eccessiva conservazione dei dati	9,6	3,68	DETTAGLI

Premendo il pulsante "DETTAGLI" si aprirà una nuova scheda che indicherà, per ogni minaccia, le misure di sicurezza ad essa relativa e la misura in cui essa è stata applicata. Premere il pulsante "OK" per tornare alla scheda di "Sintesi del rischio".

Premendo sul pulsante 

si verrà riportati alla scheda "Criteri di impatto" e sarà possibile modificare le risposte da quella scheda in poi.

- **CONSULTAZIONE PREVENTIVA:** scheda in cui è possibile definire se è necessario richiedere o meno una consultazione preventiva all'autorità garante.

Come indicato nell'articolo 36 comma 1 del Regolamento "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."
Ciò significa che, se la DPIA restituisce un risultato non soddisfacente circa l'attenuazione del rischio da parte delle misure di sicurezza applicate, è possibile richiedere una consultazione preventiva, cioè una richiesta di controllo da parte del Garante che potrà bloccare il trattamento o autorizzarlo.
Per le comunicazioni agli interessati ed al Garante si vedano le specifiche sezioni.

INFORMATIVA PER IL TRATTAMENTO DEI DATI PERSONALI NEWS LETTER

Covar 14, in qualità di titolare del trattamento, intende informarLa in merito al trattamento dei Suoi dati personali ai sensi dell'**articolo 13** del Reg Eu 16/679.

1.Finalità del trattamento

Il Suo indirizzo mail è richiesto al fine di ricevere informazioni sui servizi pubblici erogati svolta da Covar14 mediante la newsletter.
Il conferimento dei dati, in particolare l'indirizzo mail, è facoltativo, tuttavia, il rifiuto a fornire i propri dati comporta l'impossibilità a ricevere informazioni in merito alle attività svolte da Covar14.

2.Base giuridica

L'invio della newsletter potrà avvenire solo con il Suo consenso.

3.Modalità per il trattamento dei dati:

I suoi dati verranno trattati utilizzando strumenti manuali nonché strumenti informatici anche mediante l'inserimento di essi in banche dati, elenchi e liste idonei alla memorizzazione, gestione e trasmissione dei dati, nei modi e nei limiti necessari al perseguimento delle predette finalità.
I Suoi dati saranno trattati da persone specificatamente autorizzate al trattamento dei dati personali.

4.Responsabile del trattamento:

Il servizio di newsletter viene effettuato attraverso la Società IDM nominata, per tale ragione, responsabile del trattamento.
Ai dati potrebbero accedere (per finalità di assistenza al sito, agli applicativi, alla rete informatiche e per la connettività) nostri tecnici incaricati o consulenti esterni nominati questi ultimi responsabili del trattamento.

5.Diritti degli interessati

Lei in qualità di interessato ha diritto in qualunque momento di esercitare il diritto di accesso, di rettifica, alla cancellazione, alla limitazione del trattamento, alla portabilità, di opposizione, scrivendo al Titolare del trattamento al seguente indirizzo:
infoedatabreach@covar14.it specificando l'oggetto della sua richiesta, il diritto che intende esercitare e allegando fotocopia di un documento di identità che attesti la legittimità della richiesta.

6.Conservazione dei dati

Il Titolare del trattamento conserva i dati personali sino a revoca del consenso. Qualora intendesse revocare il consenso, i suoi dati, per la finalità indicata al punto 1 verranno cancellati.

7.Revoca del Consenso

Lei ha diritto in qualsiasi momento a revocare il proprio consenso cliccando su cancella iscrizione presente sulla news letter ricevuta o sul sito nella sezione dedicata alla newsletter.

8.Responsabile Della Protezione

La Società COVAR 14 ritenendo di primaria importanza la tutela dei dati personali degli interessati, ha nominato un responsabile della protezione dei dati (DPO) che potrà essere contattato scrivendo all'indirizzo mail dpo@covar14.it per ogni tematica riguardante la protezione dei dati personali.