DATA 19/05/2021

PROT. N° 470/2021

RIF. N°

REGOLAMENTO DI ANALISI

SULLA SICUREZZA E TRATTAMENTO DEI DATI

(GDPR 2016/679/UE)

MODELLO ORGANIZZATIVO PRIVACY

Approvato in prima versione con determinazione n. 17/2018 dell'Amministratore Unico di ATR il 25.05.2018
Aggiornamento versione n. 2 con determinazione n. 31/2019 dell'Amministratore Unico di ATR il 01.08.2019
Aggiornamento versione n. 3 con determinazione n.19/2021 dell'Amministratore Unico di ATR il 19.05.2021

[Versione n. 3 del 19.05.2021]

INDICE

1 PREMESSA

Il presente documento, adottato da ATR - società consortile a responsabilità limitata (di seguito per brevità ATR) conformemente al GDPR 2016/679/UE (REGOLAMENTO DEL PARLAMENTO EUROPEO relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati), in materia di protezione dei dati personali (anche con riferimento alle categorie dei dati particolari e dei dati giudiziari) trattati con l'ausilio di strumenti elettronici o manuali, ha lo scopo di fornire un quadro, il più possibile strutturato, del sistema privacy adottato e delle conseguenti azioni volte a garantire la *compliance* alla normativa privacy. Tali azioni mirano a contenere, entro limiti accettabili, il rischio di: distruzione, anche accidentale (perdita della disponibilità), accesso non autorizzato (compromissioni dell'integrità e della riservatezza), trattamento non consentito o non conforme alle finalità della raccolta, dei dati personali in possesso di ATR.

Definisce i criteri organizzativi, procedurali e tecnologici per la gestione della sicurezza in merito al trattamento dei dati personali, sensibili e/o giudiziari, le figure chiave della privacy previste dalla normativa: formalità e attribuzione di compiti. Vengono identificate le misure di natura organizzativa e tecnologica atte a garantire il raggiungimento ed il mantenimento nel tempo, dei livelli di sicurezza ritenuti adeguati per la salvaguardia delle informazioni trattate e delle risorse gestite da ATR.

2 VALIDITÀ E DESTINATARI DEL DOCUMENTO

Il presente documento ha validità fino a che non insorgano importanti modifiche organizzative, tecniche, procedurali o legislative. In tali casi deve essere revisionato onde assicurare un adeguato livello di sicurezza ai dati personali, rapportato alle differenti categorie, in relazione alle eventuali variazioni del livello di rischio a cui gli stessi sono soggetti e ad eventuali modifiche della tecnologia informatica utilizzata dall'organizzazione.

Il Documento si applica a tutto il personale ed ai collaboratori esterni di ATR, in particolare alle funzioni aziendali incaricate di progettare ed aggiornare il piano di protezione del sistema informativo/cartaceo e di effettuare i relativi controlli.

Per i fornitori di servizi esterni all'organizzazione di ATR, è il Titolare autonomo/Responsabile del trattamento dei dati che richiede al proprio personale il rispetto delle disposizioni loro riguardanti.

3 DEFINIZIONI

Si richiama integralmente il contenuto di cui all'art. 4 del GDPR 2016/679/UE concernente la definizione dei significati attribuiti alle locuzioni rilevanti ai fini della esatta comprensione della normativa, precisandosi che per quanto non specificato nella presente sezione "definizioni" deve farsi riferimento a detta richiamata norma.

Qui di seguito si riportano, pertanto, solo le definizioni maggiormente rilevanti ai predetti fini, nonché le definizioni aggiuntive ritenute utili per la migliore comprensione del presente regolamento.

Titolare del trattamento dei dati: 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;

Responsabile del trattamento dei dati: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento

Incaricato del trattamento dei dati: la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile

D.P.O. (o R.P.D.): il responsabile della protezione dei dati designato, ai sensi dell'articolo 37 del GDPR, dal Titolare del trattamento e/o dal Responsabile del trattamento, al quale viene affidata la sorveglianza circa l'osservanza del presente regolamento e delle disposizioni normative dell'unione e dello Stato Italiano, al quale vengono attribuite le prerogative ed assegnati i compiti di cui agli articoli 38 e 39 del GDPR

Interessato: la persona fisica identificata o identificabile a seguito della raccolta dei dati; si precisa che alle persone giuridiche non è attribuibile la qualità di interessato

Amministratore di Sistema: figura professionale è finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti e/o amministratore di basi di dati, di reti e di apparati di sicurezza e/o di sistemi software complessi

Dati personali: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dati particolari: i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

Dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

Dati giudiziari: dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza

Dato anonimo: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile, può essere trattato senza il consenso da parte dell'interessato. **(pseudonimizzazione)**

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

Comunicazione: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione

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

Banca di dati: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Misure di sicurezza: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione adottato dal Titolare del trattamento, dal Responsabile del trattamento, o suggerito dal D.P.O.

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico, ed indipendentemente che sia costituito in formato cartaceo o informatizzato ho in entrambe le predette modalità

Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile

Consenso dell'interessato: 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

Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati

Strumenti elettronici: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento, l'insieme degli strumenti elettronici e delle procedure per la verifica dell'identità o della dichiarazione di identità

Sistemi di videosorveglianza: i sistemi elettronici per la visione di immagini attraverso strumenti di ripresa sia fissi che con la possibilità di "zoom", con la possibilità di registrare tali immagini per il tempo previsto dalla vigente normativa e dalle disposizioni dell'Autorità di Controllo

Credenziali di autenticazione: i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati dal sistema di autenticazione informatica per la verifica dell'identità o di una dichiarazione di identità

Parola chiave: componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica

Profilo di autorizzazione: l'insieme dei dati cui una persona può accedere, nonché dei trattamenti ad essa consentiti

Sistema di autorizzazione: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente

Cookies: stringhe di testo di piccole dimensioni che i siti visitati dall'utente inviano al suo terminale (solitamente al browser), dove vengono memorizzati per essere poi ritrasmessi agli stessi siti alla successiva visita del medesimo utente.

4 DESCRIZIONE DI ATR

4.1 Struttura organizzazione interna

A seguito della conclusione di un complesso ed articolato processo riorganizzativo, meglio descritto sia nel piano triennale di prevenzione della corruzione sia nel modello organizzativo generale recentemente adottato da ATR in adeguamento al disposto normativo di cui al decreto legislativo n. 231/2001 sulla responsabilità degli enti, oggi ATR non agisce sulla base di una pianta organica definita, essendosi invece dotata di una organizzazione "flat", in base alla quale le esigenze operative vengono di volta in volta pesate e distribuite dal Coordinatore Generale ai dipendenti secondo criteri di competenza, opportunità, sostenibilità, anche in relazione ai tempi di realizzazione. Sulla base di tale organizzazione "flat", pertanto, si è superata una rigida ripartizione delle competenze fra gli addetti di ATR, potendo le funzioni aziendali essere oggetto di scambio tra i diversi dipendenti, fatta eccezione per il personale impiegato per il controllo della sosta, le cui funzioni non ricadono nella riferita organizzazione "flat" ma consistono gli specifici compiti di sorveglianza della sosta regolamentata. In questo modo all'interno di ATR tutti i dipendenti concorrono allo svolgimento delle attività istituzionali dell'azienda, ivi compresa la gestione dei fascicoli cartacei ed informatizzati; in tal modo essi sono altresì direttamente coinvolti nel trattamento dei dati personali necessari al corretto sviluppo di detta attività gestionale, divenendo direttamente responsabili della conformità del loro operato ai principi di legalità e, necessariamente, al corretto trattamento delle banche dati.

4.2 Politiche aziendali

ATR, pur avendo dedicato particolare attenzione al tema del corretto trattamento dei dati personali, sia in sede di gap analisys sia in sede di conseguente approntamento delle misure di sicurezza ritenute idonee a prevenire possibilita' di illecito o non conforme trattamento, è perfettamente consapevole che il margine di rischio non può essere azzerato ma solo congruamente ridotto in sede di analisi prognostica, il che tuttavia lascia un margine residuo di possibili inconvenienti e correlate azioni risarcitorie e/o sanzionatorie.

Ciò premesso ATR ha ritenuto opportuno, in un'ottica di responsabile e consapevole gestione delle risorse pubbliche ad essa conferite, prevedere un progressivo accantonamento annuale, in caso di avanzo di gestione, atto a garantire alla stessa una disponibiltà economica in ipotesi in cui venga chiamata a rispondere, a fronte di eventuali responsabilità, sia da parte dell'autorità di controllo sia da parte di terzi. Tale accantonamento verrà appostato in bilancio sotto il nome di "Accantonamento privacy".

ATR inoltre si riserva di verificare sul mercato assicurativo l'offerta di prodotti intesi a coprire il sopra evidenziato rischio; laddove tali coperture saranno possibili e compatibili con le risorse aziendali, ATR provvederà ad accendere le relative polizze, e a liberare gli eventuali accantonamenti nel frattempo effettuati.

5 RUOLI E RESPONSABILITÀ PER IL TRATTAMENTO DEI DATI PERSONALI

Il “Codice in materia di protezione dei dati” (GDPR 2016/679/UE) individua alcune “figure chiave” soggettive cui sono attribuiti specifici obblighi e diritti in relazione all’attività di trattamento dei dati personali.

ATR in ossequio alla normativa di riferimento, ha adottato un “Funzionigramma Privacy” (allegato 1) nel quale sono illustrate le linee gerarchiche (funzionali e di staff) che fanno capo ai ruoli privacy istituiti all’interno di essa, unitamente alle figure che trattano banche dati sensibili (sorveglianza sanitaria e sicurezza sul lavoro), al fine di consentire il corretto assolvimento di tutti gli adempimenti previsti dal Codice, e di cui si riporta nel seguito una breve descrizione.

5.1 Titolare del Trattamento dei dati

Titolare del trattamento dei dati (Capo IV GDPR 2016/679/UE) è ATR nel suo complesso, nella persona del Suo Legale Rappresentante.

I principali compiti del Titolare del trattamento dati sono quelli di mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento; a tal fine il Titolare del trattamento deve:

1. assumere tutte le decisioni in ordine alle finalità ed alle modalità del trattamento, ivi compreso il profilo della sicurezza;
2. procedere al censimento dei dati trattati ed all’individuazione della tipologia dei trattamenti effettuati sugli stessi ed effettuare, se necessario, la notificazione al Garante;
3. procedere all’individuazione ed alla nomina scritta del Responsabile del trattamento, degli eventuali Incaricati del trattamento dei dati e fornire loro il codice identificativo e la credenziale di autenticazione ed idonee istruzioni scritte in ordine alle modalità di trattamento;
4. provvedere alla nomina del D.P.O.;
5. assicurarsi che il D.P.O. eserciti efficacemente la propria attività di vigilanza, anche tramite verifiche periodiche, sulla puntuale osservanza da parte degli Incaricati delle istruzioni impartite e delle vigenti disposizioni in materia di trattamento dei dati;
6. assicurarsi che il D.P.O. eserciti periodicamente la propria attività di vigilanza sulle attività degli Amministratori di sistema, attraverso gli *access log file* disponibili o altre metodiche di garanzia;
7. attuare gli obblighi di informazione ed acquisizione del consenso, quando richiesto, nei confronti dell’interessato;
8. adottare tutte le misure di sicurezza idonee per il trattamento dei dati sulla base di un criterio di responsabilità e di responsabilizzazione dei vari attori della privacy aziendale;
9. Garantire a tutti gli incaricati la corretta informazione e formazione sul tema della privacy e delle sue applicazioni in ATR;
10. redigere il Regolamento sulla Sicurezza e provvedere periodicamente al suo aggiornamento;
11. riferire all’Assemblea dei Soci nella relazione accompagnatoria del bilancio d’esercizio, dell’avvenuta redazione o aggiornamento del presente Regolamento.

12. nel caso di affidamento all'esterno di alcune attività di trattamento dei dati deve, anche avvalendosi del Responsabile del trattamento dei dati:
    a) valutare la posizione del soggetto esterno;
    b) verificare i contratti che disciplinano l'affidamento all'esterno dei servizi connessi al trattamento dei dati, valutandone la compatibilità e la congruenza con il GDPR 2016/679/UE;
    c) provvedere a formalizzare per iscritto tutte le istruzioni ed i compiti;
    d) provvedere, qualora ne ricorrano i presupposti, dichiarare la contitolarità del trattamento, definendo congiuntamente con il contitolare le finalità ed i mezzi del trattamento, in conformità a quanto stabilito dall'art. 26 del GDPR 2016/679/UE

5.2 Responsabile del trattamento dei dati

Nella struttura organizzativa interna di ATR, il ruolo di Responsabile del trattamento dei dati (art. 28 del GDPR 2016/679/UE) è ricoperto dal Coordinatore Generale in qualità di referente per la privacy.

Per la sorveglianza sanitaria e la sicurezza sul lavoro dei lavoratori, tale ruolo è ricoperto rispettivamente dal Medico Competente e dal Responsabile del Servizio di Prevenzione e Protezione.

I principali compiti del Responsabile del trattamento sono:

1. provvedere alla predisposizione ed alla tenuta del registro trattamento dati, di cui all'art. 30 del GDPR 2016/679/UE, conformandolo alle indicazioni ivi previste al primo e secondo comma; al riguardo si evidenzia che ATR è un'azienda pubblica con un numero di dipendenti largamente inferiore ai 250; pertanto si ritiene di unificare in un unico documento, a cura del Responsabile del Trattamento, le previsioni previste al primo e secondo comma di detto art. 30;
2. informare prontamente il Titolare di ogni questione rilevante ai fini della protezione dei dati personali/sensibili;
3. curare il coordinamento di tutte le operazioni di trattamento dei dati personali/sensibili sulla base delle istruzioni scritte impartite dal Titolare;
4. operare in sinergia con il Titolare per l'attuazione degli obblighi di informazione ed acquisizione del consenso, quando richiesto, nei confronti dell'interessato;
5. procedere alla nomina scritta degli Incaricati del trattamento dei dati e fornire loro il codice identificativo e la credenziale di autenticazione ed idonee istruzioni scritte in ordine alle modalità di trattamento;
6. promuovere lo svolgimento di un continuo programma di informazione/formazione e addestramento degli Incaricati del trattamento e mantenere attivo un programma di controllo e monitoraggio della corrispondenza con le regole di sicurezza;
7. gestire e coordinare tutte le attività legate alla sicurezza sia dei soggetti interni, sia degli eventuali soggetti esterni (*outsourcer*);
8. operare per l'effettuazione delle verifiche del livello di conformità riguardo a tutti gli adempimenti organizzativi, procedurali e di sicurezza previsti dal GDPR 2016/679/UE e relazionarne al Titolare;

9. per quanto attiene l’assolvimento degli obblighi generali di sicurezza, annualmente individuare/aggiornare le misure preventive e protettive atte alla eliminazione/diminuzione dei rischi identificati, sottoporne l’elenco al Titolare e, in base alle sue indicazioni, predisporre il programma di attuazione particolareggiato di tali misure;
10. operare in sinergia con il Titolare per l’aggiornamento del Registro del Trattamento e del Regolamento Privacy sulla sicurezza dei dati;
11. verificare, nel caso di affidamento delle attività di trattamento a soggetti giuridici esterni, i contratti che disciplinano l’outsourcing, valutandone la compatibilità e la congruenza con il GDPR 2016/679/UE;
12. adottare le misure idonee a consentire all’Interessato l’effettivo esercizio dei diritti previsti dall’art. 12 del GDPR 2016/679/UE, e garantire detto esercizio;
13. evadere senza ritardo le eventuali richieste avanzate dagli interessati ai sensi dell’art. 15 del GDPR 2016/679/UE;

5.3 Responsabile della Protezione dei Dati (R.P.D. o D.P.O.)

ATR non rientra tra i soggetti elencati dall’art. 37, primo comma, per i quali la nomina di un D.P.O. è di carattere obbligatorio; nemmeno tratta sistematicamente dati particolari o giudiziari, e neppure compie trattamenti sistematici su larga scala (c.d. big data) che rendo obbligatoria l’individuazione tale figura.

Tuttavia ATR intende ugualmente dotarsi di un D.P.O., a maggiore garanzia della liceità ed idoneità del trattamento, nonché al fine di rendere più agili i rapporti con l’autorità di controllo e garantire l’indipendenza di tale funzione di interfaccia.

A tale fine, considerate le ridotte dimensioni di ATR, e stante la sopra accennata organizzazione di carattere “flat” dell’organigramma aziendale, si è ritenuto non incompatibile affidare le funzioni di D.P.O. allo stesso Responsabile del Trattamento, il quale peraltro, identificandosi nella figura del Coordinatore Generale, offre idonee garanzie di indipendenza e di autonomia.

Viene messo a disposizione del D.P.O. un budget annuale peri ad € 5.000,00, che egli potrà utilizzare per il raggiungimento delle finalità attribuitegli dalla normativa; tale budget verrà annualmente ripristinato solo per la parte effettivamente utilizzata, utilizzo che dovrà essere rendicontato al Titolare del Trattamento.

Al D.P.O. vengono affidate le seguenti funzioni:

1. informare e fornire consulenza al titolare del trattamento, agli eventuali contitolari, nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal presente regolamento, dal regolamento 2016/679/UE nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

2. sorvegliare l'osservanza del presente regolamento, dal regolamento 2016/679/UE nonché di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o degli eventuali contitolari del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

3. fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;

4. cooperare con l'autorità di controllo;

5. fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del regolamento 2016/679/UE, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

6. effettuare a campione e senza preavviso alcuno, controlli sulle attività degli Amministratori di sistema, verificando le modalità e finalità di accesso ai dati in consultazione. In caso di lieve Non Conformità suggerirà imediatamente inecessari correttivi. In caso di grave Non Conformità, ne darà immediata comunicazione al Titolare del Trattamento per quanto questi riterrà di competenza.

Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

5.4 Incaricati del Trattamento dei dati

Incaricati del trattamento dei dati sono tutti i dipendenti che abbiano accesso ai dati personali di qualunque categoria (ordinari, particolari, giudiziari) in forma cartacea o informatica.

L’incarico è affidato per iscritto dal Responsabile del trattamento dei dati mediante lettera di nomina che individua puntualmente l’ambito del trattamento consentito.

Ciascun Incaricato opera con responsabilità propria, rispettando le prescrizioni emesse dal Responsabile del Trattamento dati assumendo, in ordine al trattamento dei dati, le seguenti responsabilità:

1) svolgere le attività previste dai trattamenti attenendosi strettamente alle istruzioni impartite dal Responsabile del Trattamento dati ed alle prescrizioni di sicurezza contenute nel Documento di Analisi sulla Sicurezza dei dati;
2) non effettuare attività di trattamenti non consentite o non previste nell’ambito del suo ruolo aziendale senza l’esplicita autorizzazione del Responsabile del trattamento;
3) usare la massima riservatezza e discrezione durante le operazioni di trattamento dei dati e nella conseguente loro protezione;
4) rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
5) evitare i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta, in armonia con gli obblighi derivanti dal regolamento 2016/679/UE;
6) informare il Responsabile Trattamento dati in caso di diminuzione del livello di sicurezza che coinvolga dati personali.

5.5 Amministratori di sistema

Viene definito quale "amministratore di sistema" colui che, in ambito informatico, ha una competenza professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti e/o amministratore di basi di dati, di reti e di apparati di sicurezza e/o di sistemi software complessi.

L'Amministratore di sistema, pur non essendo preposto ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), svolge, nella Sua consueta attività, in molti casi, specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

Attività tecniche quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "in chiaro" le informazioni medesime.

L'Amministratore di sistema" ha il compito di:

1. interfacciarsi con il Responsabile per quanto riguarda l'implementazione/aggiornamento delle politiche e delle procedure di sicurezza previste per la gestione dei sistemi informativi;
2. assicurare la corretta applicazione delle politiche, procedure e standard di sicurezza predisposte per la manutenzione hardware e software;
3. consentire all'Incaricato l'autonoma modifica della parola chiave al primo utilizzo del software di gestione della banca dati, ove ciò sia tecnicamente possibile, e successivamente almeno ogni sei mesi, nel caso di trattamento di dati personali, e almeno ogni tre mesi, nel caso di trattamento di dati sensibili e di dati giudiziari;
4. disattivare le credenziali di autenticazione non utilizzate da almeno sei mesi, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica, in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali;
5. configurare i profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sulla base delle indicazioni fornite dal Responsabile del trattamento dei dati ed in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento;
6. periodicamente, e comunque almeno annualmente, verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione;
7. proteggere i dati personali e gli elaboratori utilizzati per il trattamento degli stessi contro il rischio di intrusione e dell'azione di *malicious program*, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale;
8. aggiornare periodicamente i programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici ed a correggerne difetti;
9. definire in accordo con il Coordinatore Generale la pianificazione delle attività atte a evitare violazioni interne o esterne;
10. effettuare il salvataggio dei dati sensibili e/o giudiziari, presenti sulle unità di storage centralizzate, con frequenza almeno settimanale e secondo le istruzioni organizzative e tecniche impartite dal Responsabile del trattamento dei dati;

11. verificare l'integrità dei supporti di memorizzazione prima dell'utilizzo e procedere alla loro distruzione nel caso in cui non possano essere più riutilizzati;

12. proporre l'adeguamento dei sistemi (HW e SW) a livelli tecnologici tali da garantire la disponibilità del servizio;

13. prevedere e svolgere attività di controllo sull'operato di personale esterno ad ATR per interventi di installazione, aggiornamento e manutenzione HW e SW;

14. collaborare con il Responsabile del trattamento dei dati alla stesura/aggiornamento del Documento Programmatico sulla Sicurezza.

6 VIDEOSORVEGLIANZA

I dati raccolti mediante i sistemi di videosorveglianza devono essere protetti con idonee e preventive misure di sicurezza tecniche ed organizzative a tutela del trattamento dei dai personali degli interessati.

A seguito della necessità di tutelare il patrimonio aziendale, che può essere sottoposto a rischi di perdita di valore e/o distruzione per atto vandalico, evento calamitoso e/o malavitoso, per la sicurezza del lavoro e quale ulteriore misura di sicurezza predefinita fin dalla progettazione del sistema privacy, l'azienda ha ritenuto necessario ed opportuno addivenire, previa consultazione della RSA con la supervisione dei rappresentanti di categoria a livello territoriale, alla sistemazione e funzionamento di un servizio di videosorveglianza, definito mediante l'apposizione di telecamere presso:

1. sede aziendale interno uffici e parcheggio esterno,
2. biglietteria di Cesenatico,
3. alcuni parcheggi in struttura di Cesena,

In merito al punto 1. e 2. le telecamere sono collegate ad un sistema di rilevazione e registrazione delle immagini sul server sito nella sala macchine aziendale. Essendo le telecamere in ambienti di lavoro, è stato sottoscritto apposito accordo con le OOSS con tutte le specifiche a tutela dei lavoratori.

In merito al punto 3, parte del sistema è affidato alla Parcheggi S.p.A di Cesena, con la quale ATR ha sottoscritto un regolare Contratto di manutenzione ed assistenza.

6.1 Adempimenti

Sono stati apposti idonei cartelli segnaletici e la registrazione viene conservata per un tempo non superiore alle n. 72 ore consecutive, prima della sovra scrittura.

Per la funzione di videosorveglianza è stata definita la figura di amministratore di sistema e solo il Responsabile del trattamento ne può prendere visione, nel rispetto del principio di liceità, proporzionalità e non eccedenza.

Il dettaglio delle banche dati e dei rispettivi profili di autorizzazione, che individuano le specifiche attribuzioni, sono state riportate nel "Registro del Trattamento" (Allegato 4), che costituisce parte integrante del presente documento.

7 ANALISI DEL RISCHIO

Il Titolare del trattamento ha ritenuto opportuno adottare misure di sicurezza idonee a ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o trattamento dei dati personali non consentito o non conforme alle finalità della raccolta.

In particolare, il Titolare ha adottato le misure di sicurezza che ha ritenuto indispensabili a garantire un livello minimo di sicurezza per tutti i trattamenti in essere; ha adottato inoltre misure specifiche di maggiore garanzia in presenza di trattamento di eventuali dati particolari, nonché in presenza di aree di rischio maggiormente elevate.

Detta valutazione e le conseguenti misure sono riportate in apposita sezione del registro del trattamento dati (Allegato 4).

Appare necessario, dunque, identificare ed implementare le misure di sicurezza maggiormente idonee a garantire la protezione dei dati, ovvero quelle misure determinate in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento.

Tale valutazione non può prescindere da un'attività di Analisi dei Rischi volta a:

- classificare i dati in base al loro livello di criticità/rischio;
- analizzare le minacce e le vulnerabilità del sistema informativo;
- identificare ed implementare le contromisure maggiormente idonee a garantire un livello di sicurezza adeguato per la protezione dei dati particolari di dati personali.

7.1 Metodologia utilizzata

In questa sezione vengono descritti i criteri adottati da ATR nella conduzione dell'analisi di rischio, al fine di proteggere i dati personali sensibili e/o giudiziari.
In considerazione della contenuta struttura organizzativa di ATR, non si è ritenuto di considerare, quale ulteriore parametro di possibile aggravamento del rischio, il numero di persone che concorrono al trattamento della medesima banca dati, ritenendosi di valutare tale rischio irrilevante o comunque scarsamente rilevante, in quanto il massimo delle persone che possono essere coinvolte nel medesimo trattamento, non supera, di norma, le 3-4 unità (vedi Allegato 4).

Il livello di rischio si esprime, pertanto, come combinazione di due soli parametri:

- la gravità delle conseguenze di eventi, espressa in termini di impatti tangibili o intangibili;
- la relativa probabilità stimata di accadimento, determinata su base annuale,

come nell'immagine di seguito riportata:

P = Probabilità di accadimento

G = Gravità delle conseguenze

R = Livello di rischio = P x G

Nella rappresentazione dei rischi, i livelli di probabilità e gravità possono essere assegnati su base storica o su valutazioni di natura prevalentemente qualitativa o, qualora siano disponibili idonei dati statistici, in forma quantitativa, con riferimento alla schematizzazione riportata nelle successive tabelle 1 e 2.

Convenzionalmente le probabilità e gravità dei rischi, vengono assegnati in base a scale per numeri interi variabili da 0 a 3.

Tabella 1: attribuzione delle classi di probabilità dei rischi

Punteggio	Livello	Descrizione
3	**Alto**	Probabilità di accadimento dell'evento considerata stimata superiore a 5 casi su base annuale.
2	**Medio**	Probabilità di accadimento dell'evento considerata stimata tra i 3 e i 5 casi, su base annuale.
1	**Basso**	Probabilità di accadimento dell'evento considerata stimata in 1 evento su base annuale.
≅ 0	**Nullo o trascurabile**	Probabilità di accadimento dell'evento considerata stimata in 0 eventi su base annuale.

Tabella 2: attribuzione della gravità d'impatto dei rischi

Punteggio	Gravità d'impatto	Descrizione
3	**Molto critica**	Gravi impatti o conseguenze gravi
2	**Significativa**	Impatti significativi
1	**Bassa**	Impatti limitati
≅ 0	**Nulla o trascurabile**	Impatto nullo o trascurabile

Le classi di rischio risultanti, sono rappresentati nella tabella 3.

Tabella 3: Classificazione degli indici di rischio

Indice di rischio	Classificazione degli indici di rischio e delle azioni suggerite	
R > 6	**Alto**	È una condizione non accettabile, per la quale è richiesta una sensibilizzazione al più alto livello di management coinvolto, un rafforzamento delle azioni di prevenzione e protezione in essere nel sistema di gestione, un'adeguata destinazione di risorse destinate al controllo della efficace attuazione delle misure adottate.
3 < R ≤ 6	**Medio**	È una condizione non accettabile, che richiede una sensibilizzazione a livelli appropriati del Coordinatore Generale, un adeguamento delle azioni di prevenzione e protezione in essere nel sistema di gestione,
1 ≤ R ≤ 3	**Basso**	È una condizione accettabile, in quanto richiede una sostanziale conferma delle misure organizzative già previste nel sistema di gestione, integrata al più da una sensibilizzazione del Coordinatore Generale e dal monitoraggio delle relative attività.
R = 0	**Nullo o trascurabile**	Rischio trascurabile o nullo: non richiede alcuna azione.

7.2 Risultati dell'attività

Lo svolgimento dell'attività di analisi dei rischi ha condotto ATR all'identificazione del livello di rischio calcolato su una scala di valori stimata in Alto, Medio, Basso, Nullo o trascurabile, cui i beni sono potenzialmente esposti.

A tal fine, ATR ha effettuato un checkup delle proprie banche dati, provvedendo contestualmente ad individuarne:

- ✓ La tipologia di banca dati;
- ✓ L'ufficio/funzione ove sono allocate;
- ✓ La tipologia di dati contenuti (Dati Particolari o Ordinari);
- ✓ Il tipo di formato (cartaceo, elettronico);
- ✓ I programmi utilizzati per la loro elaborazione;
- ✓ Le locazioni ove fisicamente sono ubicate le macchine;
- ✓ Il livello di rischio;
- ✓ Le misure adottate per ridurre o eliminare il rischio,
- ✓ Categoria degli interessati,
- ✓ Destinatari,
- ✓ Durata massima del trattamento.

Gli esiti dell'analisi sono stati riportati nel "Registro del Trattamento", oggetto di verifica ed aggiornamento annuale.

8 MISURE DI SICUREZZA CONTRO IL RISCHIO DI DISTRUZIONE/PERDITA DEI DATI (D.P.I.A.)

In questa sezione, vengono descritte le contromisure di sicurezza fisiche, logiche ed organizzative adottate da ATR, per fronteggiare il rischio di distruzione/perdita dei dati trattati.

8.1 Misura Organizzativa

Sono stati nominati gli Amministratori di Sistema.

L'Amministratore di Sistema, si occupa dell'installazione, configurazione, gestione/manutenzione, aggiornamento e monitoraggio del sistema informatico presente in Azienda.

Il principale obiettivo è quello di gestire l'hardware e il software del sistema affinché essi funzionino in modo corretto e l'insieme dei servizi offerti dal sistema informativo possa essere erogato nella maniera più efficiente possibile agli utenti.

L'hardware e il software oggetto dell'attività dell'Amministratore di Sistema sono tutti quelli presenti ed operativi in Azienda.

I nominativi di tali figure, le loro competenze e i software ed hardware per i quali sono stati nominati, sono stati riportati in Allegato 2, oggetto di verifica ed aggiornamento a cura del Responsabile del trattamento dati.
All'interno della lettera di nomina standard vengono altresì definite le misure logiche, tecniche ed organizzative che permettono al titolare al trattamento dati di verificare periodicamente il corretto operato dei singoli amministratori nominati.

8.2 Sistemi di sicurezza fisica

Tutta la sede di ATR, che occupa interamente il piano secondo dell'edificio, è dotata di estintori ad anidride carbonica per l'utilizzo delle apparecchiature informatiche nel rispetto della legge sulla sicurezza nel lavoro.

Le macchine server sono collocate in un apposito locale (Server Farm), il cui accesso è riservato al personale autorizzato.

La sala server è dotata di:

- Impianto di condizionamento ambientale, opportunamente dimensionato;
- Impianto elettrico a norma e ridondante per i server "*mission-critical*";
- Gruppo di continuità atto a garantire una permanenza stabile dell'energia elettrica erogata. Ciò allo scopo di consentire, in conseguenza di un'improvvisa assenza di energia, l'autonomia temporale necessaria al corretto spegnimento dei server/apparati;

8.3 Dispositivi di emergenza e prevenzione della perdita dei dati

I server, in base alla criticità dei servizi che svolgono, sono dotati di sistemi ridondanti:

- doppio processore;
- doppio alimentatore;
- dischi del sistema operativo in *mirroring* (RAID 1) e dischi dati in RAID 5 - 10.

In caso di *failure* hardware questa configurazione permette di limitare/evitare l'interruzione dei servizi, la perdita di dati e consente un eventuale rapido ripristino degli stessi.

Per scongiurare il rischio di danni hardware o perdite di dati dovuti ad improvvisa mancanza di energia elettrica è operativa una procedura di gestione UPS che in caso di blackout consente ai server la chiusura delle applicazioni più critiche, il salvataggio dei dati in corso di modifica e lo spegnimento corretto degli apparati.

8.4 Misure di sicurezza contro il rischio di distruzione da incendio

ATR ha predisposto un idoneo Piano di emergenza secondo la normativa specifica in ambito di prevenzione incendi.

All'interno di ATR sono presenti addetti alla squadra di emergenza che sono stati debitamente formati al loro compito in relazione alla valutazione del rischio incendio determinata in base al D.M. 10/03/98 ed al D.Lgs 81/2008 e s.m.i..

In tale ottica, sono previste periodiche visite ispettive interne per identificare:

1. la presenza ed efficienza dei vari presidi antincendio;
2. la loro semplice fruibilità;
3. la informazione e formazione impartita ai collaboratori in caso di emergenza;
4. l'effettuazione della simulazione di evacuazione in condizioni di emergenza.

Si da atto che i documenti cartacei contenenti dati particolari sono contenuti in idonei uffici, a cura degli incaricati alla loro custodia, con chiusura a chiave ed accesso controllato.

8.5 Sistema antivirus

I server e tutti gli elaboratori sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-*quinquies* del codice penale mediante un sistema antivirus centralizzato con aggiornamento periodico e automatico dei file delle impronte virali e distribuzione delle stesse a tutti i *client.*

L' antivirus è operativo a 3 livelli:

- Livello Server, al quale viene controllato ogni file che transita sui server;
- Livello Mail Server, a cura del fornitored el servizio (Aruba) al quale viene controllata la posta elettronica prima di distribuirla;
- Livello Client.

8.6 Servizi antispam

È operativo un servizio Antispam sul mail server, a cura del fornitore del servizio (Aruba) che filtra la posta elettronica non voluta evitando il suo recapito ai destinatari. Questo tipo di messaggi elettronici sono frequente causa di sovraccarichi dei server e veicolo di attività non sicure da parte degli utenti del sistema.

8.7 Sistema di back up dei dati

È attivato un sistema di backup quotidiano centralizzato e automatizzato di tutti i documenti presenti sui server, la cui gestione è regolata come segue:

- Sono definiti i volumi logici o le aree di disco da sottoporre a backup, sui vari server;
- a ciascun utente viene assegnata una directory, in un'area disco di un server che sia sottoposta a backup, dove mantenere i dati in maniera sicura. L' accesso a queste directory è consentita esclusivamente all'utente proprietario, nonché agli Amministratori del backup.

- I dati sottoposti a backup vengono trasferiti giornalmente su un dispositivo NAS collocato nella sala server ATR. Almeno una volta al mese una copia dei dati prsenti nel disposizitvo NAS viene copiata su un dispositivo magneto-ottico rimovibile e trasferita in un edificio separato da quello che ospita i server che contengono tali dati.

9 MISURE DI SICUREZZA CONTRO IL RISCHIO DI ACCESSO NON AUTORIZZATO

In questa sezione, vengono riportate le misure di sicurezza definite da ATR sulla base dei dettami del Codice e dei risultati dell'attività di analisi dei rischi, per fronteggiare i rischi di accesso non autorizzato alle informazioni.

9.1 Protezione delle aree e dei locali

Per l'accesso alla sede di ATR è necessario essere autorizzati all'ingresso dalla segreteria.

Le stanze degli uffici sono protette da porte dotate di chiave. Armadi e cassettiere presenti all'interno degli uffici sono dotati in gran parte di alloggiamenti dotati di chiusura a chiave nei quali archiviare i documenti più riservati. La custodia di tali chiavi è affidata al singolo dipendente.

Il locale (Server Farm) che ospita le macchine server e tutti gli apparati di rete, è protetto da porte dotate di chiave, custodite a cura degli Amministratori di sistema e del Responsabile del trattamento

L'accesso alla sala server è consentito al Responsabile del trattamento e all'Amministratore di sistema, o alle persone espressamente autorizzate. In assenza del personale autorizzato, la sala server deve essere tenuta chiusa a chiave.

9.2 Sistema di autorizzazione e autenticazione

Il processo di autenticazione consente di ottenere uno specifico insieme di privilegi di accesso ed utilizzo, denominato profilo, rispetto alle risorse del sistema informatico. I profili di autorizzazione, per ciascun Incaricato o per classi omogenee di Incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

A ciascun profilo è associato un gruppo di utenti, che condividono gli stessi privilegi di accesso e utilizzo.

In base all'organigramma e all'aggiornamento dello stesso vengono conseguentemente aggiornati i privilegi di utilizzo del sistema informatico.

La funzione Sviluppo Tecnologico assegna la prima password al dipendente di nuova assunzione, il quale sarà responsabile del suo cambiamento al primo log-in.

La password associata a uno specifico username, per l'accesso alla rete di ATR, ha una durata di 60 giorni e viene richiesto l'aggiornamento in automatico allo scadere del sessantesimo giorno. La password richiesta deve avere almeno 8 caratteri.

La password di autenticazione alla rete è composta da almeno 8 (otto) caratteri, oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito, e non deve derivare dal nome utente o dai dati personali dell'utente.

Gli applicativi utilizzati per il trattamento possono sfruttare l'autenticazione effettuata sulla rete, oppure richiedere a loro volta un nome utente e una password.

Nome utente e password sono strettamente personali e l'Incaricato è tenuto:

a. a non comunicare a terzi le password;

b. a non annotare le password su supporti posti in vicinanza della propria postazione di lavoro, o comunque incustoditi;

c. ad attenersi a tutte le indicazioni.

Le credenziali di autenticazione sono disattivate:

- nel caso in cui non vengano utilizzate da almeno 6 (sei) mesi, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
- in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

9.3 Controllo degli accessi

È presente un sistema di controllo degli accessi basato principalmente sulle seguenti politiche di gestione delle password:

- tutte le postazioni di lavoro sono protette da una password di accesso;
- la password di accesso va modificata con cadenza almeno bimestrale;
- ai fini dell'assistenza sistemistica, la password di accesso può venire comunicata agli incaricati, e sostituita al termine dell'intervento.

Per proteggere l'accesso da Internet alla LAN è attivato 1 (uno) firewall.

Tutte le porte in entrata sui firewall sono chiuse, salvo quelle richieste da alcuni servizi conosciuti e controllati.

Ove possibile il traffico dati in entrata verso la LAN è instradato tramite VPN che, pur sfruttando la rete Internet, consente il passaggio dei dati attraverso un "tunnel" criptato.

9.4 Registrazione degli accessi a sistemi, applicazioni e basi dati

Esiste un processo di controllo e verifica della sicurezza del sistema informatico, mediante l'utilizzo di strumenti automatici di registrazione a livello di sistema, di gestione delle basi dati e di applicazioni.

L' accesso degli utenti agli applicativi critici nonché le attività, svolte dagli stessi, classificate come potenzialmente idonee a compromettere la sicurezza del sistema informativo di ATR vengono, ove tecnicamente possibile, registrate e controllate attraverso le attività degli amministratori di sistema;

Gli eventuali problemi riscontrati sono riportati al Responsabile del trattamento che procede all'individuazione delle opportune azioni correttive.

9.5 Utilizzo e riutilizzo dei supporti di memorizzazione

I supporti rimovibili contenenti dati sensibili e/o giudiziari possono essere riutilizzati da altri Incaricati, non autorizzati al trattamento degli stessi dati, solo se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

I supporti rimovibili contenenti dati sensibili e/o giudiziari se non utilizzati sono distrutti o resi inutilizzabili

Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati (vedi documento "Istruzioni per gli Incaricati")

10 MISURE DI SICUREZZA CONTRO IL RISCHIO DI TRATTAMENTO NON CONSENTITO E/O NON CONFORME

In questa sezione, vengono riportati i criteri definiti dall'organizzazione sulla base dei dettami del Codice e dei risultati dell'attività di analisi dei rischi, per fronteggiare i rischi di trattamento non consentito.

10.1 Personale autorizzato al trattamento dei dati

La designazione degli Incaricati è effettuata per iscritto e deve individuare puntualmente l'ambito del trattamento consentito.

In caso di dimissioni di un Incaricato del trattamento o di revoca delle autorizzazioni al trattamento dei dati, il Responsabile del trattamento dei dati deve darne immediata comunicazione all'Amministratore di sistema di competenza che provvederà a disattivare la possibilità di accesso al sistema per il soggetto in questione.

Sono impartite, dal Responsabile all'Incaricato, istruzioni operative per il trattamento dei dati e istruzioni tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare trattamenti non consentiti dei dati.

10.2 Verifiche periodiche delle condizioni per il mantenimento delle autorizzazioni

L'Amministratore di sistema verifica annualmente le autorizzazioni di accesso alle banche dati oggetto del trattamento e se necessario, provvede a variare i profili di autorizzazione, confrontandosi sempre con il Responsabile del trattamento.

11 MISURA PER IL RISCHIO DI INDISPONIBILITÀ DEI DATI

In questa sezione, vengono descritti i criteri e le modalità per il ripristino della disponibilità dei dati, a seguito di distruzione o danneggiamento, definite da ATR sulla base dei dettami del Codice e dei risultati dell'attività di analisi dei rischi.

11.1 Criteri per il ripristino dei dati

Nel caso di trattamento di dati devono essere adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici.

Nel caso di trattamento di dati particolari il ripristino deve avvenire in tempi certi compatibili con i diritti degli interessati e non superiori a 7 (sette) giorni.

ATR è in grado di garantire, quanto previsto nei due commi precedenti, stante le misure sopra descritte ai paragrafi 8 e 9 che si richiamano.

11.1.1 Danneggiamento dell'hardware

Nell'eventualità che si danneggino in modo disastroso uno o più componenti hardware di un Server, necessari al suo funzionamento, si interverrà tempestivamente per ripristinare i servizi nel più breve tempo possibile procedendo secondo le seguenti modalità:

- Eventuale spostamento temporaneo dei servizi non operativi su un altro Server, tenendo in considerazione i tempi e gli oneri di un tale intervento;
- Sostituzione immediata delle parti danneggiate se presenti in Azienda come parte di ricambio, oppure

acquisto delle parti presso il produttore e invio delle stesse tramite corriere espresso;

Se il danno hardware riguarda le unità di memorizzazione di massa (hard disk) si intraprenderanno le seguenti ulteriori azioni:

- Valutazione relativa alla possibile perdita di dati, strettamente legata alla presenza o meno di sistemi Raid;
- Se non vi è stata perdita di dati, e questa potrebbe verificarsi a seguito della non operatività del sistema Raid, si procederà a valutare l'effettuazione dello spegnimento dei relativi servizi e di un backup supplementare delle informazioni, al fine di non esporre i dati a ulteriori rischi;
- Se si verifica una perdita di dati è necessario eseguire un immediato backup di tutte le informazioni rimaste, valutando se è maggiormente produttivo procedere a un tentativo di recupero dei dati persi, ripristinare lo stato del sistema utilizzando un backup effettuato in precedenza o intervenire con una combinazione di entrambi i tipi di attività;

Nel caso in cui la non disponibilità dei servizi sia causa di malfunzionamenti software, è necessario:

- Ripristinare nel più breve tempo possibile i servizi isolando la causa del problema, valutando l'eventuale momentanea sospensione di altri sistemi in conflitto;
- Installare nuovamente o spostare su altri Server il servizio non disponibile, valutando costi ed oneri che tale attività implica.

11.1.2 Intrusioni nel sistema informatico

Si richiamano le misure descritte ai precedenti paragrafi 8 e 9.

Nel caso si verifichino intrusioni dall'esterno o dall'interno nel sistema informatico si adotteranno le seguenti attività e modalità:

- Dettagliato studio dei file di log prodotti dagli apparati hardware e dai sistemi software che proteggono l'accesso alla rete aziendale, al fine di reperire informazioni utili all'individuazione dell'intruso e alla definizione delle modalità d'attacco attuate;
- Precisa analisi dei file di log generati dagli applicativi e dai sistemi presenti su ogni server, in modo da verificare quali attività sono state intraprese dall'intruso e a quale rischio (sottrazione, manomissione, visualizzazione, ecc.) sono stati esposti i dati aziendali;
- Nel caso in cui non sia possibile interrompere l'accesso non autorizzato al sistema o non sia possibile evitarne ulteriori, si provvederà alla sospensione eventuale dei servizi hardware/software che rendono possibile l'attacco in corso o che hanno consentito l'intrusione ormai conclusa;
- Realizzazione di tutte le contromisure necessarie ad evitare futuri attacchi del medesimo tipo: l'analisi delle modalità d'intrusione, a cui si è fatto riferimento sopra, è in questo senso fondamentale.

11.1.3 Modalità di dismissione di hardware obsoleto

Se si rende necessario dismettere il disco rigido e/o memorie di massa di strumenti informatici che contenga o possa avere contenuto dati personali e/o sensibili e/o giudiziari, si adotteranno le seguenti attività e modalità:

- La funzione Sviluppo Tecnologico preleva il dispositivo guasto/obsoleto e provvede a rendere non più utilizzabile fisicamente il supporto ,oppure, quando non è possibile distruggere il supporto, si procede alla cancellazione sicura dei dati dal dispositivo, utilizzando apposito software di "Data Shredder" che effettua cancellazioni multiple.

11.1.4 Modalità di gestione degli account di posta per assenza dell'incaricato

In caso di assenze programmate (es. ferie o attività di lavoro fuori sede), ATR mette a disposizione di ciascun incaricato apposite funzionalità di sistema (accesso da remoto alla webmail) per consentire di inviare automaticamente messaggi di risposta contenenti le coordinate (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura.

In caso di eventuali assenze non programmate (es: per malattia), qualora il lavoratore non possa attivare la procedura sopra descritta, il Titolare del trattamento, perdurando l'assenza oltre 7 giorni, se necessario e attraverso l'operato degli Amministratori di Sistema, dispone l'attivazione della sopra citata procedura, avvertito l'interessato.

Se un incaricato al trattamento dei dati dovesse rimanere assente dal lavoro improvvisamente o per un lungo periodo e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, viene consentita la possibilità di delegare a collega di fiducia o, se non possibile, consentito all'Amministratore di Sistema, a verificare il contenuto di messaggi e a inoltrare al Responsabile del trattamento, per conto del Titolare, quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa, informando il lavoratore alla prima occasione utile.

11.1.5 Modalità di gestione degli account di posta per dimissioni o licenziamento dell'incaricato

Dal ricevimento della comunicazione mail da parte dell'Ufficio Personale con i riferimenti del lavoratore dimesso o licenziato per giusta causa, gli Amministratori di Sistema provvedono a:

- impostare un risponditore automatico per consentire di inviare automaticamente messaggi di risposta contenenti le coordinate (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura.
- disabilitare l'account di posta entro due mesi dalla data delle dimissioni o del licenziamento.

11.1.6 Modalità di gestione dei documenti di lavoro

Relativamente ai file aziendali residenti sul PC o sul server gestiti dal lavoratore assente, dimesso o licenziato, il Responsabile del trattamento deciderà a quale altro incaricato assegnarne l'utilizzo.

12 SICUREZZA NELL'OUTSOURCING

In questa sezione, vengono descritti i criteri e le modalità per garantire l'adozione delle misure di sicurezza in caso di *outsourcing* delle attività di trattamenti di dati.

Il Titolare può decidere di affidare il trattamento di alcune banche dati (riguardanti ad es: elaborazione buste paga, videosorveglianza, medicina del lavoro, servizio prevenzione e protezione, ecc.), a soggetti terzi esterni all'organizzazione di ATR. Questi ultimi, in virtù del contratto sottoscritto e delle condizioni contrattuali (privacy

e riservatezza) in esso contenute, possono assumere la veste di Titolari autonomi, Contitolari o Responsabili esterni del trattamento.

Tali qualità verranno definite di volta in volta, in relazione ai singoli trattamenti affidati, sulla base delle corrispondenti lettere di incarico nelle quali verranno specificate i trattamenti o le parti di trattamento affidati.

Nell'Allegato 3 vengono indicati i soggetti in outsorcing con le corrispondenti funzioni di rispettiva competenza. Tali soggetti sono tenuti al rispetto autonomo del GDPR 2016/679/UE qualora Titolari o Contitolari; saranno tenuti al rispetto delle indicazioni di ATR qualora Responsabili esterni del trattamento.

Il Titolare autonomo ed il Contitolare del trattamento sono tenuti a comunicare ad ATR che sono state adottate le misure idonee di sicurezza per il trattamento dei dati di ATR secondo quanto disposto dalla vigente normativa, e che il trattamento verrà effettuato in conformità alla stessa.

13 FORMAZIONE E SENSIBILIZZAZIONE

In questa sezione, vengono descritti i criteri e le modalità per svolgere l'attività di sensibilizzazione e informazione/formazione del personale di ATR, come previsto dalla normativa di riferimento.

13.1 Pianificazione degli interventi formativi

La formazione viene programmata al momento dell'ingresso in servizio, nonché in occasione di cambiamenti

di mansioni, o di introduzione di nuovi e significativi strumenti operativi, rilevanti rispetto al trattamento di dati personali.

ATR al fine di ottemperare a quanto stabilito dal GDPR pianifica annualmente il corso di formazione e sensibilizzazione in materia privacy, il cui scopo è quello di rendere edotto tutto il personale incaricato al trattamento di dati personali:

- dei rischi che incombono sui dati;
- delle misure disponibili per prevenire eventi dannosi;
- dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività;
- delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure di sicurezza adottate dal Titolare.

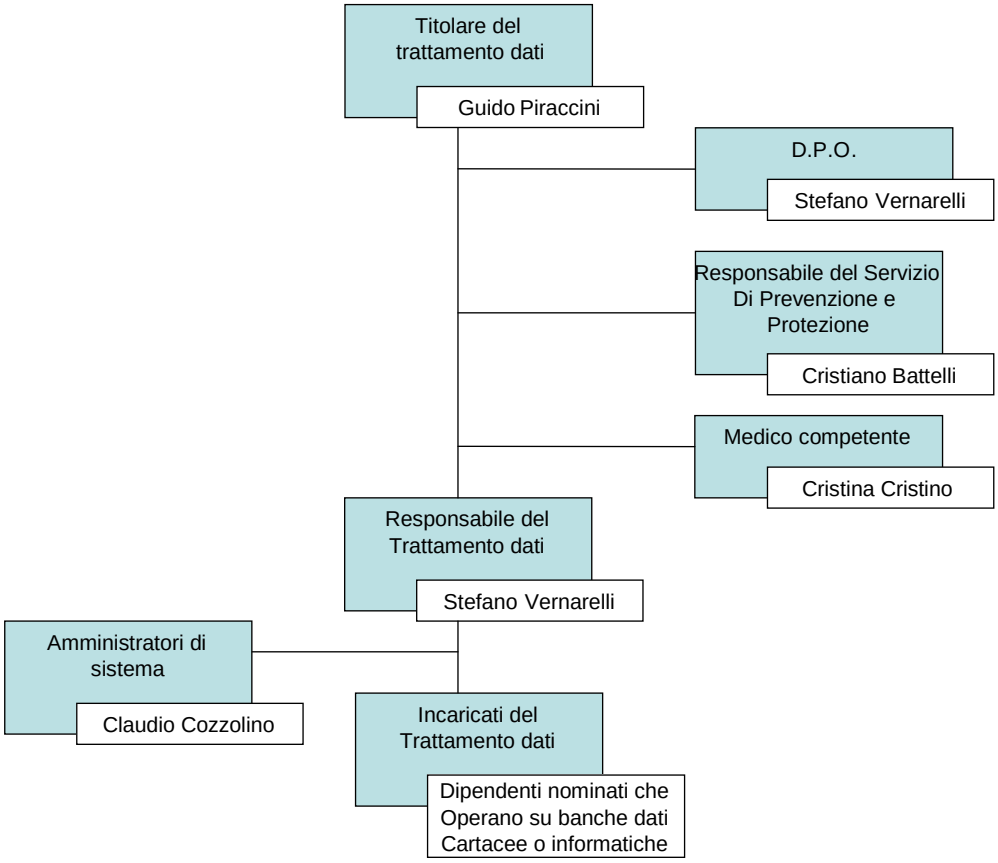
La progettazione del Piano di Formazione di ATR e la realizzazione degli interventi formativi in esso contenuti, contribuiscono a diffondere efficacemente le risultanze dell'attività di analisi dei rischi, le politiche e le procedure di sicurezza adottate dall'organizzazione, e le modalità di utilizzo corretto degli strumenti informatici, minimizzando la componente, sempre presente, di resistenza al cambiamento.

Cesena, 19/05/2021

Il Titolare del trattamento dei dati – ATR

_____

ALLEGATO 1 – FUNZIONIGRAMMA PRIVACY



ALLEGATO 2– ELENCO DEGLI AMMINISTRATORI DI SISTEMA

Cognome	**Nome**	**Funzione aziendale**	**Software e Hardware gestiti**
Cozzolino	Claudio	Resp. Operativo Sviluppo Tecnologico	Tutti i sistemi installati e le banche dati operanti in ATR (vedi Allegato 4 al presente regolamento)