CASIRATE GAS 2 S.R.L.

MANUALE GESTIONE PRIVACY IN CONFORMITA' AL REGOLAMENTO UE 679/2016

Versione 1.1 – Maggio 2018

Redazione a cura di:

Emiliani dott. Ettore

ECA

Indice

ECA

1. Il nuovo Regolamento UE 679/2016

1.1 Iter di attuazione

Il nuovo Regolamento Europeo - Regolamento (UE) 2016/679 del Parlamento Europeo (L. 119) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati è stato pubblicato sulla GUUE del 04 maggio 2016. Il Regolamento Europeo (di seguito indicato come "Regolamento UE" o come "GDPR") è direttamente applicabile e vincolante in tutti gli Stati membri e non richiede una legge di recepimento nazionale, fatta eccezione per alcuni ambiti sui quali rimanda, deroga o richiede l'integrazione regolatoria dei singoli Stati. La diversa forma dell'atto – da Direttiva a Regolamento, risponde alla primaria volontà del legislatore europeo di porre sullo stesso piano tutti gli Stati membri, garantendo medesimi diritti e doveri, assicurando uniformità alla protezione dei dati personali e certezza al diritto. Il Regolamento UE è stato approvato il 27 aprile 2016, entrato in vigore il 25 Maggio dello stesso anno ma destinato ad avere piena attuazione dal 25 Maggio 2018, data a partire dalla quale abrogherà la Direttiva 95/46/CE del Parlamento europeo e del Consiglio, 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (c.d. Direttiva Madre). Nonostante il differimento temporale della piena efficacia del GDPR alcune sue parti ne richiedono immediata applicazione, pertanto fino al 24 maggio 2018, è necessario considerare due atti normativi regolatori: la Direttiva Madre, quindi per l'Italia, il Decreto Legislativo n. 196/2003 (Codice in materia di dati personali) e il Regolamento UE.

1.2 Cosa cambia con il nuovo regolamento

Il Regolamento UE cambia profondamente la prospettiva in cui si colloca la protezione dei dati personali sebbene a una prima lettura possa rispecchiare una impostazione simile a quella della Direttiva Madre rispetto al costrutto portante (informativa, finalità, consenso), ai ruoli, ai diritti degli interessati e ai doveri dei titolari e dei responsabili. Il GDPR consacra il diritto alla protezione

dei dati personali come diritto fondamentale e costituzionale configurandolo come diritto alla autodeterminazione informativa. Questo è un principio portante fondato dalla Direttiva, che il Regolamento UE eredita, ma di cui ne ridisegna radicalmente l'implementazione passando dalla logica dell'adempimento prevalentemente formale ad un approccio regolatorio fortemente sostanziale e centrato sulla responsabilità di assicurare/mantenere la conformità al regolamento nonché di tutelare i diritti e la dignità degli interessati. Il Regolamento UE, inoltre, traccia il passaggio da un diritto alla protezione dei dati personali di tipo nazionale/individuale ad un diritto di tipo europeo/sociale. In generale il GDPR collocandolo in questa premessa e provando a dimensionarlo su diritti-doveri-controllo:

a) muta l'approccio regolatorio da "formale e reattivo" in "sostanziale e proattivo", il trattamento e la protezione dei dati personali evolvono nell'acquisire una propria e autonoma rilevanza all'interno dei processi organizzativi e gestionali;
b) consolida le garanzie e i diritti azionabili dall'interessato per il controllo delle proprie informazioni e l'esercizio dell'autodeterminazione ereditati dalla Direttiva, riaffermandone molti (diritto all'accesso, rettifica, cancellazione, limitazione, revoca e opposizione); rafforzandone altri - in primis la disciplina del consenso del quale introduce un vera e propria definizione dell'istituto del consenso esplicito, e della trasparenza rispetto alla quale perfeziona il catalogo delle informazioni da esporre nell'informativa; introducendone di nuovi (diritto alla portabilità, all'oblio, all'opposizione verso il trattamento di profilazione);
c) accresce le responsabilità del titolare e del responsabile con la positivizzazione del principio di accountability con la finalità di porre chi tratta i dati personali in una posizione di ridurre i rischi di operazioni non conformi o non consentite motivando, in tal senso, il titolare e il responsabile a comportamenti e prassi virtuose;
d) centralizza la governance e il controllo sul rispetto e la conformità dei trattamenti alla normativa, tramite la cooperazione e la valorizzazione delle Autorità di Controllo nazionali; incoraggiando meccanismi di

certificazione; ampliando il sistema vigilanza; rafforzando quello sanzionatorio sia nelle specifiche comuni che nelle misure applicative.

1.3 Ambito di territorialità

Il regolamento (considerando da 14 a 27, art. 3) si applica al trattamento dei dati personali da parte di titolari anche non stabiliti nel territorio dell'Unione purché il trattamento riguardi l'offerta di beni, servizi o il monitoraggio del comportamento del soggetto interessato aventi luogo nell'Unione.

1.4 Accresciuta responsabilità dei titolari e dei responsabili del trattamento

La responsabilità dei titolari (art. 24 e 25), e del responsabile (art. 28) **si configura come una sostanziale assunzione di rischio**, atteso che il titolare deve mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, la conformità del trattamento al regolamento tenendo conto, della natura, dell'obbligo, del contesto e delle finalità di trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le liberà delle persone fisiche. A titolari e responsabili di trattamento si affianca una nuova figura obbligatoria per le pubbliche amministrazioni: il responsabile della protezione dei dati personali (c.d. "data protection officer"). Prioritariamente rientrano tra le responsabilità del Titolare e dei Responsabili: l'attuazione delle prassi di privacy by design/default, la valutazione d'impatto, la definizione e il mantenimento delle procedure di sicurezza e valutazione dei rischi, la tenuta dei rispettivi registri delle attività di trattamento, la valutazione prudenziale sulla violazione dei dati personali, del coefficiente di gravità e delle relative ricadute sul soggetto interessato. In dettaglio ruolo e obblighi dei titolari e dei responsabili sono descritti al successivo paragrafo.

1.5 Rafforzamento delle tutele riservate all'interessato

Nel nuovo Regolamento è rafforzata l'introduzione delle misure di sicurezza e delle misure di tutela e garanzia dell'interessato nel trattamento dei suoi dati, sin dalla progettazione degli strumenti utilizzati. In particolare, sono previsti i seguenti obblighi:

a. **Privacy by design - considerando 78) art. 25 comma 1**

ECA

Attiene le buone prassi di protezione dei dati personali sin dalla progettazione del trattamento. Le misure strumentali a tale scopo sono:

i) la migliore applicazione del principio di minimizzazione dei dati personali oggetto del trattamento con riferimento tanto alla quantità dei dati, tanto ai tempi di conservazione e ai livelli di accessibilità, tanto alle prefissate finalità;
ii) la pseudonimizzazione ovvero l'oscuramento dei dati identificativi del soggetto interessato;
iii) definizione di dati personali e tempi strettamente necessari al trattamento, in relazione alle diverse finalità.

b. Privacy by default - considerando 78) art. 25 comma 2

Il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita (di default), solo i dati personali necessari per ogni specifica finalità del trattamento (che non risultino pertanto eccedenti rispetto al ruolo del soggetto che li tratta). Sarà quindi di fondamentale rilevanza curare, le diverse autorizzazioni di lettura e di modifica dei dati (in relazione ai diversi profili dei soggetti autorizzati al trattamento), curando adeguatamente anche eventuali procedure organizzative interne.

c. Valutazione di impatto (DPIA) - considerando da 89 a 96, art. 35, 36

La valutazione d'impatto precede il trattamento ed è volta a compensare particolari probabilità e gravità di rischio. Viene richiesta per trattamenti su larga scala, con incidenza su un vasto numero di interessati, con un elevato rischio connesso all'introduzione di nuove o particolari tecnologie, all'implementazione di trattamenti di profilazione o di sorveglianza o all'utilizzo di particolari dati. L'Autorità di controllo redige e pubblica l'elenco di tipologie di trattamenti soggetti a preventiva valutazione di impatto. La valutazione di impatto deve contenere almeno:

- una descrizione sistematica dei trattamenti previsti, delle finalità e l'eventuale ricorrenza di un legittimo interesse;

- la valutazione sulla necessità e la proporzionalità dei trattamenti rispetto alle predefinite finalità;
- la valutazione dei rischi per i diritti e le libertà degli interessati;
- le previste misure organizzative e tecniche (comprese quelle di sicurezza) e ogni meccanismo ritenuto utile per la tutela dei diritti dei soggetti interessati.

La responsabilità della valutazione d'impatto attiene prioritariamente il Titolare supportato dal Responsabile protezione dai dati. Si rende necessaria in caso di revisione tecnologica, per i trattamenti di larga scala, e per i trattamenti espressamente indicati dall'Autorità di controllo.

d. Sicurezza e valutazione dei rischi - considerando 83, 84, art. 32

Il regolamento prevede misure di sicurezza idonee da adottare in relazione alla valutazione dei rischi. Titolare e responsabile sono tenuti tanto alla valutazione dei rischi quanto all'adozione delle misure che comprendono: la pseudonimizzazione, la cifratura; misure implementative della riservatezza, dell'integrità, della disponibilità delle informazioni; la resilienza dei sistemi e delle applicazioni di trattamento nonché il loro tempestivo ripristino in caso di incidente fisico o tecnico. Le misure vanno contemperate allo stato dell'arte, ai costi di attuazione, alla natura, al contesto e alla finalità di trattamento. Alcuni indicatori di rischio (soprattutto connessi ai trattamenti informatizzati) sono declinati nella definizione di violazione di dato personale.

e. Violazione dei dati personali e relativa notifica - considerando da 85 a 88, art. 4, 33, 34

Il regolamento declina la violazione dei dati personali affiancando alla tradizionale componente dolosa quella accidentale prevedendo pari implicazioni. La violazione del dato personale viene definita come 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. Il titolare deve comunicare all'Autorità di Controllo l'avvenuta violazione dei dati personali trattati entro e non oltre 72 ore dall'acquisizione della conoscenza dell'accadimento descrivendone la natura della violazione, le categorie e il numero

approssimativo degli interessati e del numero di registrazioni dei dati personali in questione; i dati di contatto del responsabile della protezione dei dati; le probabili conseguenze della violazione; le misure adottate o che si intendono adottare per rimediare la violazione o attenuarne gli effetti negativi. Nel caso in cui sia determinato un Responsabile, tale soggetto deve informare il Titolare nel caso di avvenuta violazione di dati personali da lui trattati. Oltre alla comunicazione all'Autorità di Controllo, la violazione deve essere comunicata anche all'interessato se la violazione è suscettibile di elevati rischi per i diritti e le libertà dell'interessato (art. 34 del GDPR).

f. Introduzione dei registri delle attività di trattamento – considerando 82, art. 30.

Il titolare e il responsabile di trattamento devono tenere i rispettivi registri delle attività. Il registro del titolare deve contenere: riferimenti di contatto del titolare, del rappresentante del titolare del trattamento nell'Unione e del responsabile della protezione dei dati; le finalità; descrizione degli interessati e dei destinatari; la categoria dei dati personali trattati; la presenza di trasferimenti di dati verso un Paese Terzo un'organizzazione internazionale unitamente alla documentazione sulle appropriate garanzie; la tempistica della cancellazione dei dati; la descrizione della misure di sicurezza e organizzative adottate. Il registro del responsabile deve contenere oltre alle due ultime voci previste ed elencate per il registro del titolare: i riferimenti di contatto dei responsabili, dei titolari per conto dei quali operano, dei rappresentanti e del responsabile della protezione dei dati; le categorie dei trattamenti effettuati per conto del titolare.

g. Smaltimento di dispositivi e supporti contenenti dati personali

Permane l'obbligo di garantire la protezione dei dati anche mediante un'accurata cancellazione al momento della distruzione dei supporti che li contengono. Sul tema, si segnala un provvedimento dell'Autorità Garante su "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali" - 13 ottobre 2008 - G.U. n. 287 del 9 dicembre 2008.

1.6 Diritti dell'interessato

Il consenso deve essere: libero, specifico, informato e inequivocabile; non è ammesso il consenso tacito o presunto. Deve essere reso e manifestato attraverso dichiarazione o azione positiva inequivocabile e concludente (come la selezione di un'apposita casella in un sito web, la scelta di specifiche impostazioni tecniche o qualsiasi altra dichiarazione o comportamento che indichi chiaramente la volontà dell'interessato di accettare il trattamento proposto). Non è richiesta necessariamente la forma scritta anche se questa risulta essere la modalità più idonea ad accertare che il consenso sia stato inequivocabilmente fornito e che sia esplicito. Si precisa che nel caso il trattamento richieda il consenso, il titolare dovrà essere in grado di dimostrare inequivocabilmente di averlo ottenuto. Per il trattamento di dati sensibili (il GDPR parla di categorie particolari di dati) è necessario il consenso (art.9 comma 2 lettera a)) a meno che il trattamento non sia necessario per la tutela di diritti di grado superiore dell'interessato stesso o pubblici o di terzi, oppure per obbligo di legge, qualora l'interessato non sia in grado di fornire il consenso (art. 9 comma 2 lettere c, f, g, i, j).

Informativa – considerando da 58 a 73, art. 12, 13, 14

Il titolare del trattamento è tenuto a fornire l'informativa all'interessato, indipendentemente dall'obbligo di acquisire il consenso, salvo il caso in cui l'interessato sia già in possesso delle informazioni (art. 13 co. 4) o in altri casi particolari descritti nel regolamento (art. 14 co. 5).

Contenuti dell'informativa

Il titolare del trattamento è tenuto a informare il soggetto interessato in merito a:

- identità e dati di contatto del titolare del trattamento, del suo rappresentante e del responsabile della protezione dei dati personali;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento ed i legittimi interessi perseguiti dal titolare del trattamento o da terzi (qualora sia basato sull'art. 6, paragrafo 1, lettera f) del GDPR);

- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali e, nel caso in cui i dati personali non siano raccolti presso l'interessato, anche le categorie di dati trattati e le relative fonti di provenienza;
- l'eventuale intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso di trasferimenti di cui all'articolo 46 e 47, o all'articolo 49, comma 2, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stai resi disponibili;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- i diritti azionabili dall'interessato comprendenti: l'accesso ai dati personali, la rettifica o la cancellazione degli stessi, la limitazione del trattamento o l'opposizione; oltre al diritto alla portabilità dei dati; la revoca del consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; il diritto di proporre reclamo a un'autorità di controllo;
- la necessità di comunicare i dati personali in base a un obbligo legale o contrattuale oppure se si tratta di un requisito necessario per la conclusione di un contratto, nonché la natura obbligatoria o facoltativa del conferimento, nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative circa la logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

A riguardo si segnalano alcuni punti di attenzione:

- Deve essere chiarito l'eventuale trasferimento di dati in un paese terzo (ad esempio nel caso di utilizzo di servizi cloud). Si

ricorda che anche per tali servizi è responsabilità del titolare garantire la sicurezza dei dati e le modalità di accesso da parte dell'interessato.

- Rispetto alla normativa previgente, occorrerà garantire – in specifici casi - la limitazione del trattamento dati e la portabilità dei dati.
- La necessità di indicare eventuali processi automatici di profilazione e le conseguenze per l'interessato di tale trattamento dati.

Si precisa che:

- nel caso in cui i dati siano raccolti presso l'interessato, il titolare del trattamento che intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento, dovrà fornire all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente
- nel caso in cui i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento che intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento, potrà non fornire l'informativa all'interessato qualora risulti impossibile o farlo implicherebbe uno sforzo sproporzionato in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici e fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di rendere l'informativa rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In questo caso, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni.

Il GDPR contiene inoltre indicazioni specifiche per i casi nei quali i dati non siano stati ottenuti presso l'interessato: oltre alle informazioni richieste nell'informativa all'art. 13, sarà necessario indicare la fonte da cui hanno origine i dati personali e se si tratta di una fonte di pubblico accesso.

Caratteristiche dell'informativa

Il regolamento specifica in dettaglio le caratteristiche espositive dell'informativa, che deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; veicolata da un linguaggio chiaro e semplice, soprattutto nel caso in cui gli interessanti siano minori. Per agevolare la comprensione, il regolamento incoraggia l'utilizzo di icone in combinazione con la forma estesa per presentare i contenuti dell'informativa in forma sintetica, icone che dovranno essere identiche in tutta l'Ue e dovranno essere definite dalla Commissione. Una maggiore comprensione e chiarezza dell'informativa si potrebbe altresì ottenere mediante la redazione di più informative che si differenzino, ad esempio, in relazione alle diverse categorie di interessati e/o servizi resi loro disponibili.

Indicazioni pratiche per la stesura dell'informativa

Dal punto di vista pratico, tenendo conto delle indicazioni di cui sopra, si possono individuare le seguenti linee guida:

a. Articolare l'informativa su più livelli, per garantire che:
    - le informazioni di base siano subito presentate all'interessato e risultino di immediata lettura e comprensione,
    - maggiori dettagli siano consultabili dagli interessati scegliendo sezioni di approfondimento.
b. Per agevolare la consultazione l'informativa può essere articolata sulla base dei profili degli utenti, prevedendo ad esempio contenuti specifici per le differenti categorie, ciascuna potenzialmente caratterizzata da differenti trattamenti dei dati personali
c. Garantire che l'informativa descriva non solo i trattamenti di dati personali visualizzabili dall'utente mediante gli applicativi software (sicuramente più vicini alla percezione dell'utente) ma anche quelli trattati per attività

connesse all'erogazione dei servizi informatici, effettuati dai sistemi e spesso non direttamente visibili agli utenti

d. Garantire che nel suo complesso l'informativa fornita agli interessati soddisfi i requisiti di completezza previsti dalla normativa
e. Per i trattamenti che presentano un alto profilo di rischio per le libertà dell'interessato, potrebbe essere opportuno tenere traccia esplicita dell'avvenuta consultazione dell'informativa da parte degli utenti ed eventualmente dare evidenza dei cambiamenti intervenuti sulla stessa nel caso di cambiamenti.

Per agevolare la stesura dell'informativa, si riportano nell'Allegato 2 informazioni aggiuntive ed esempi.

Diritti "tradizionali" – considerando da 58 a 73, art. 12 a 17

I diritti azionabili dall'interessato già previsti dalla Direttiva e dal Codice, oltre a quello di ricevere idonea informativa riguardano: il diritto di accesso, la rettifica, la cancellazione, l'opposizione al trattamento. Tra le novità previste nel nuovo GDPR rispetto alla Direttiva 95/46/CE e al Codice Italiano si citano:

- il riscontro deve essere fornito senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Nel caso di diniego, il riscontro deve essere fornito al più tardi entro un mese dal ricevimento della richiesta
- la definizione da parte del titolare di eventuali oneri sull'interessato nei casi particolari previsti nell'art. 12 comma 5.

A differenza della normativa previgente, è posto meno l'accento sul riscontro da fornire all'interessato per quanto attiene le modalità del trattamento: viceversa è posto l'accento su altri elementi come, ad esempio, il periodo di conservazione e le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi. Si precisa inoltre che, la risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

Nuovi Diritti: diritto di limitazione; diritto di opposizione alla profilazione; diritto alla cancellazione, all'oblio; diritto alla portabilità; – art. 18, 20, 21, 22

Questi nuovi diritti estendono o rafforzano analoghi diritti presenti nella Direttiva e attuati dal Codice Italiano. Il diritto alla limitazione rappresenta un diritto diverso e più esteso rispetto al "blocco" del trattamento già previsto dal codice, in particolare, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento e quale alternativa alla cancellazione dei dati stessi, bensì anche nelle more che sia riscontrata da parte del titolare una richiesta di rettifica dei dati o di opposizione al trattamento. In condizioni di limitazione e con la sola eccezione della conservazione, ogni altro trattamento del dato è consentito solo in presenza del consenso dell'interessato, o dell'accertamento diritti in sede giudiziaria, di tutela diritti di altra persona fisica o giuridica, o in presenza di un interesse pubblico rilevante. Il diritto di opposizione alla profilazione che riconosce all'interessato il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare (legata ad esempio al proprio rendimento professionale o alla propria situazione economica, di salute, ecc…), al trattamento dei dati personali che lo riguardano compresa la profilazione. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli 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. Il diritto "all'oblio" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata nel caso questi siano stati resi pubblici on-line. I titolari hanno l'obbligo di informare della richiesta di cancellazione ogni altro titolare che tratta i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione". Inoltre l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento. Il diritto alla portabilità si applica ai dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato e solo per i dati che siano stati "forniti" dall'interessato al titolare; fanno eccezione quindi i dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare. Per tale ragione le implicazioni del Diritto di Portabilità dovrebbero

solo residualmente interessare i trattamenti dei dati personali.

1.7 Sintesi delle principali novità

Le principali novità sono sintetizzate per parole chiave nelle seguenti tabelle.

Consenso	Libero, specifico, informato, inequivocabile e concludente.
Informativa	Informazioni di contatto titolare, rappresentante e responsabile protezione dei dati; indicazione della finalità di trattamento; destinatari e categorie di dati trattati; trasferimento dati personali in paesi terzi; diritti azionabili e implicazioni; ricorrenza di altre basi giuridiche diverse dal consenso. Usabilità dell'esposizione.
Valutazione impatto	Ripensamento delle tecnologie a supporto dei trattamenti. Analisi e eventuale consultazione preventiva con l'Autorità Garante per le implicazioni sui diritti e le libertà delle persone. Obbligo del titolare, supportato dal responsabile protezione dati.
Sicurezza	Analisi dei rischi e di valutazione dell'adeguatezza delle misure tecniche e organizzative. Obbligo congiunto del titolare e del responsabile del trattamento dati.
Violazione dei dati	Equiparazione della fattispecie accidentale con quella dolosa.
Privacy by Design **Privacy by Default**	Applicazione delle tutele di trattamento sin dalla sua progettazione e avvio. Pseudonimizzazione e Minimizzazione (di dati e tempi) come garanzia e misura di PbD. Obbligo del titolare.
Responsabile PDP	Si interfaccia con le Autorità Garanti. Supporta titolare e responsabile del trattamento. Obbligatorio nelle PA.
Registro Trattamenti	Registri di competenze in cui indicare le caratteristiche, le modalità e le finalità del trattamento. Lo redigono titolare e responsabile del trattamento.
Sanzioni	Sanzioni amministrative pecuniarie fino a 20000000 EUR (per le imprese, fino al 4% del fatturato globale annuo dell'esercizio precedente)
Autorità	Comitato di controllo europeo: assicura la uniforme applicazione del Regolamento. Autorità di Controllo: autorità pubblica indipendente di uno Stato membro.

IN MERITO AI NUOVI DIRITTI	
Profilazione	L'interessato ha il diritto di non subire trattamenti automatizzati (profilazione) inconsapevoli.
Portabilità dei Dati	L'interessato ha il diritto ottenere la restituzione dei propri dati personali trasmessi e trattatati da un titolare e trasmetterli ad altri.
Oblio	L'interessato ha diritto alla de-indicizzazione o alla cancellazione delle informazioni che lo riguardano.
Sportello Unico	Unicità dell'interlocutore territoriale. Semplificazione e uniformità di gestione nell'applicazione del nuovo regolamento.

2. I soggetti del trattamento

Il GDPR individua i soggetti coinvolti nel trattamento sulla base:

1) delle finalità per le quali sono raccolti:
   - il Titolare è la persona giuridica o la persona fisica che raccoglie i dati personali per proprie finalità e decide i mezzi per il trattamento;
   - il Cotitolare è la persona giuridica o la persona fisica che condivide le finalità con altro Cotitolare e stabilisce insieme a questi le modalità di trattamento,
   - il Responsabile del trattamento è la persona giuridica o la persona fisica che esegue dei trattamenti di dati per conto del Titolare, sulla base di un contratto o altro atto giuridico,
   - il Destinatario è la persona giuridica o la persona fisica che riceve i dati dal Titolare per eseguire i trattamenti secondo le istruzioni ricevute o che esegue trattamenti per proprie finalità, nel qual caso diventa a sua volta Titolare per i trattamenti dei dati ricevuti,
   - il soggetto autorizzato è la persona fisica che ha ricevuto dal titolare precise istruzioni per l'esecuzione dei trattamenti dati di sua competenza;
   - l'interessato è la persona fisica che fornisce i propri dati personali a un Titolare per le finalità specificate nell'informativa;
2) delle caratteristiche del Titolare/Responsabile e delle tipologie e quantità di dati trattati:
   - il Responsabile della Protezione dei Dati è la persona giuridica o la

ECA

persona fisica che segue tutti i vari aspetti relativi all'applicazione del GDPR per conto del Titolare/Responsabile, deve obbligatoriamente essere presente nelle pubbliche amministrazioni;

3) dell'ambito territoriale:

- il Rappresentante nell'Unione del Titolare/Responsabile che ha la propria sede in uno stato terzo è la persona giuridica o la persona fisica che su mandato del Titolare/Responsabile funge da interlocutore per gli interessati e per le Autorità di controllo dell'Unione (ferma restando la responsabilità generale del titolare del trattamento o del responsabile del trattamento);
- l'Autorità di Controllo è la persona giuridica pubblica istituita da ogni Stato membro per sovrintendere all'applicazione e al rispetto del GDPR nell'ambito del proprio territorio;
- il Comitato Europeo per la Protezione dei Dati è la persona giuridica che a livello europeo ha il compito di coordinare il lavoro delle varie Autorità di Controllo e di supportare la Commissione.

2.1 Titolare del trattamento

Il titolare è definito all'art. 4 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". Pertanto Il Titolare non viene designato o nominato ma diventa tale al momento che raccoglie dati personali con l'intento di trattarli per finalità lecite, come previsto all'art. 6, e decide le modalità di trattamento.

Soggetto del trattamento	Titolare (definito anche "Controller")
Persona giuridica	CASIRATE GAS 2 S.R.L.
Descrizione	Il soggetto che raccoglie i dati per il conseguimento di un fine dichiarato e dispone dei mezzi per il loro trattamento. Il Titolare è responsabile del rispetto del GDPR all'interno del proprio ente e deve mettere in atto tutte le misure tecniche ed organizzative necessarie a garantire la protezione dei dati personali. Per dimostrare di aver rispettato tali obblighi il Titolare può aderire a codici di condotta o conseguire certificazioni come previsto dagli artt. 40 e 42 del GDPR.
Informazioni per l'interessato	Il titolare e all'interessato, il suo rappresentante legale devono essere resi noti.
Note	Titolare del trattamento è l'organizzazione nel suo complesso (non può essere infatti una persona fisica ed è individuata già nel Regolamento come "l'autorità pubblica" che determina le finalità e i mezzi del trattamento). Il Titolare risponde della corretta applicazione della normativa in materia di protezione dei dati personali. La distribuzione degli incarichi e delle responsabilità al suo interno sarà effettuata utilizzando gli strumenti di governo interno previsti dalla Legge o dallo Statuto e Regolamenti.

2.2 Responsabile del trattamento dati

Il GDPR definisce all'art. 4 il Responsabile del trattamento quale "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento" e ne descrive le funzioni all'art.28. Differisce dalla figura di responsabile prevista dall'attuale Codice, soprattutto per quanto concerne il rispondere in solido con il Titolare di eventuali inadempienze. Attualmente l'incarico di Responsabile del trattamento dei dati è stato assegnato internamente a coloro che ricoprono funzioni di particolare rilievo organizzativo, oltre che a soggetti esterni che eseguono trattamenti di dati per conto dell'Azienda. Certamente è necessario che l'organizzatore, quale Titolare, mantenga al proprio interno una distribuzione delle responsabilità rispetto al trattamento dati, "istruendo" opportunamente le persone che dirigono strutture interne, affinché si facciano carico dell'applicazione del GDPR nel proprio ambito, collaborando con il Titolare. La definizione di un'organizzazione interna finalizzata all'attuazione e al controllo efficace delle misure adottate per la protezione dei dati da parte del Titolare è un elemento fondamentale per poter dimostrare che il trattamento è effettuato conformemente al GDPR. Pertanto, per l'applicazione di tale disposizione risulta utile distinguere fra la funzione di "Responsabile del trattamento", così come definita all'art.28 del GDPR, assegnata a un soggetto esterno che esegue trattamenti per conto dell'Azienda e la funzione che possiamo definire di "Responsabile interno" che è assegnata a personale che ricopre funzioni di particolare rilievo organizzativo. Il responsabile esterno agisce come persona giuridica/fisica autonoma e quindi risponde in solido con il titolare di eventuali inadempienze, mentre il responsabile interno agisce per conto del titolare all'interno dell'Azienda sulla base delle competenze attribuite alla funzione organizzativa o carica istituzionale che ricopre. Possono quindi delinearsi vari scenari di distribuzione delle responsabilità interne, secondo la dimensione e la complessità della struttura universitaria. Il Responsabile del trattamento sarà quindi sempre un soggetto esterno, mentre il responsabile interno sarà un soggetto interno, opportunamente "istruito" dal Titolare riguardo alle

competenze anche decisionali in materia di protezione dei dati.

Soggetto del trattamento	Responsabile (Processor) del trattamento dati
Persona fisica	LEGALE RAPPRESENTANTE
Descrizione	Il responsabile del trattamento dati è un soggetto esterno che esegue, in base a un contratto/convenzione o altro atto giuridico, dei trattamenti di dati personali per conto del titolare e ne risponde in solido in caso di inadempienze. Al Responsabile spettano tutti i compiti del Titolare all'interno del proprio organismo (valutazione impatto, registro dei trattamenti, eventuale nomina del Responsabile della Protezione Dati, ecc.) Il Responsabile così individuato non può a sua volta nominare un altro Responsabile se non dietro autorizzazione scritta del Titolare: la catena delle responsabilità deve essere nota al Titolare. Nei contratti con sub-responsabili devono essere riportati gli stessi obblighi in materia di protezione dei dati personali previsti dal contratto tra responsabile e titolare.
Informazioni per l'interessato	Nell'informativa devono essere indicati i destinatari o le categorie di destinatari, anche interni, ai quali sono comunicati i dati per il loro trattamento. Nel caso di trasferimento di dati in un paese terzo è obbligatorio informare di ciò l'interessato e il Titolare deve verificare che il responsabile assicuri un'adeguata protezione dei dati.
Note	In azienda è considerato "Responsabile del trattamento" il soggetto terzo a cui sono affidati trattamenti per finalità. Rientrano in tale categoria per esempio i soggetti che curano applicazioni in outsourcing o in hosting per conto. Devono essere predisposte clausole contrattuali che indichino gli ambiti di responsabilità e i compiti assegnati. Il responsabile a sua volta deve garantire l'applicazione delle misure necessarie alla protezione dei dati e gli adempimenti previsti dal Regolamento. Al punto 5 dell'art. 28 è previsto che possono essere considerate garanzie sufficienti per la protezione dei dati l'adesione da parte del responsabile a codici di condotta o certificazioni approvate secondo quanto stabilito agli artt. 40 e 42 del GDPR. In caso di designazione di un sub-responsabile il responsabile conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del sub-responsabile.

2.3 Soggetti autorizzati

Nelle linee guida del Garante si afferma che "le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del regolamento", ne consegue che quanto disposto all'art. 29 del GDPR possa concretizzarsi con l'individuazione dei soggetti autorizzati al trattamento dati all'interno dell'Azienda, prima denominati "incaricati". È sottolineata l'importanza di "istruire" i soggetti, sarà quindi opportuno prevedere percorsi formativi adeguati per coloro che saranno coinvolti nel trattamento dati.

Soggetto del trattamento	Soggetti "istruiti" dal Titolare per trattare dati
Persona fisica	Collaboratori
Carica/persona fisica	Personale dipendente o collaboratori
Descrizione	Il GDPR non prevede espressamente la figura dell'incaricato del trattamento, ma all'art. 29 prescrive che l'accesso ai dati personali e i loro trattamenti devono essere effettuati da soggetti "istruiti" (in inglese è "on instructions") dal Titolare. Tale affermazione non esclude tuttavia che all'interno dell'azienda possano essere individuati coloro che sono autorizzati a effettuare i trattamenti, così come suggerito dal Garante Privacy. A tale scopo può essere individuata una organizzazione funzionale alla protezione dei dati, nella quale si delineano i vari ambiti di trattamento che competono ad ogni struttura e l'individuazione dei soggetti "incaricati" dei trattamenti secondo le afferenze, le mansioni e le responsabilità.
Informazioni per l'interessato	Nell'informativa devono essere indicati i destinatari o le categorie di destinatari, anche interni, ai quali sono comunicati i dati per il loro trattamento.

Note	Analogamente a quanto è stato fatto fino ad oggi, è possibile individuare i soggetti che sono autorizzati al trattamento dei dati, mediante una nomina individuale da parte del Titolare o Responsabile del trattamento dati, oppure individuando i trattamenti che competono all'unità organizzativa di afferenza del soggetto, che risulta pertanto incaricato per "documentata preposizione ad unità organizzativa". La necessità di prevedere la designazione per iscritto del singolo incaricato o la documentata preposizione così come concepita dall'attuale normativa, non emerge in maniera esplicita dall'art. 29 del GDPR. Il termine" istruzione" del soggetto da parte del titolare indica che è necessaria una formazione /informazione specifica alla persona per ritenerla "autorizzata" ai trattamenti di dati personali di sua competenza. Del resto, già nella disposizione "data protection by default and by design" è previsto che in fase di progettazione di un'attività, che comporti trattamenti di dati personali, debbano essere individuate le misure di sicurezza idonee alla protezione dei dati e di conseguenza anche le opportune istruzioni per gli incaricati. L'individuazione dei soggetti autorizzati al trattamento dati è una misura di sicurezza a livello organizzativo che comunque il Titolare è tenuto ad adottare. Salvo ulteriori precisazioni da parte del Garante, gli amministratori di sistema risultano essere incaricati con particolari compiti, pertanto per questa tipologia è opportuno mantenere la nomina individuale.

2.4 Responsabile della protezione dati

L'AZIENDA NON E' TENUTA ALLA NOMINA DEL RESPONSABILE PROTEZIONE DATI – IL PARAGRAFO E' COMUNQUE PREVISTO SE VOLESSE INTRODURLO COMUNQUE IN VIA CAUTELATIVA.	
Soggetto del trattamento	Responsabile della protezione dati (Data Protection Officer)
Persona giuridica/fisica	Soggetto interno/esterno
Carica/persona fisica	Persona fisica/giuridica o Gruppo di Lavoro con incarico specifico
Informazioni per l'interessato	I recapiti del RPD devono essere forniti all'interessato nell'informativa.
Note	La figura deve avere ampia autonomia. Ogni azienda valuterà in base alle proprie disponibilità e caratteristiche se affidare l'incarico a personale interno o esterno. È importante verificare che non vi siano conflitti d'interesse, ossia che il RPD nominato non debba controllare attività nelle quali è direttamente coinvolto. Sul sito del Garante sono pubblicate delle linee guida specifiche per tale figura.
Descrizione	Per l'azienda è obbligatoria la nomina di un Responsabile della Protezione Dati. L'incarico può essere affidato a personale interno o a soggetto esterno, verificando che non vi siano conflitti d'interesse. A seconda della complessità e della quantità di dati trattati, può essere individuato un team di persone che svolgono tale funzione, purché siano ben definite le mansioni e le responsabilità al suo interno. Così anche nel caso di affidamento dell'incarico a persona giuridica esterna, la quale può assolvere tale compito incaricando più persone. In questo caso, è opportuno che sia individuata una persona specifica quale punto di riferimento per l'ente. Diversamente la funzione di RPD può essere svolta per più organismi dalla stessa persona, nel caso che non sia previsto un impegno a tempo pieno. RPD agisce in autonomia (non riceve alcuna istruzione per quanto riguarda l'esecuzione di tali compiti) e funge da collegamento fra Titolare/Responsabile, gli interessati e l'autorità di controllo. I suoi compiti devono essere chiaramente definiti e devono essergli garantiti supporto, risorse e tempi di lavoro adeguati allo svolgimento della sua funzione. Nel caso di personale interno deve inoltre essergli garantita una formazione permanente per permettergli di rimanere aggiornato sugli sviluppi nel settore

	della protezione dei dati. Al RPD deve essere dato ampio accesso alle informazioni e deve essere interpellato per ogni problematica inerente la protezione dei dati e per ogni attività che implica un trattamento dati, fin dalla sua progettazione. Il RPD ha il compito di coadiuvare il Titolare/responsabile nella valutazione d'impatto e nella redazione del Registro dei Trattamenti, oltre che nella sorveglianza del rispetto del GDPR all'interno dell'Azienda. Informa e fornisce consulenza al Titolare/Responsabile e al personale interno coinvolto nel trattamento dati sull'applicazione del GDPR. Si occupa delle comunicazioni con l'autorità di controllo e con gli interessati. Nell'assolvimento dei suoi compiti il RPD non può essere penalizzato o rimosso. Le eventuali osservazioni del RPD sull'applicazione del GDPR possono essere non accolte dal Titolare/Responsabile, specificandone i motivi. La responsabilità di eventuali mancanze è comunque a carico del solo Titolare/Responsabile. Il RPD deve essere facilmente contattabile dal personale interno, dagli interessati e dall'autorità di controllo. Pertanto i suoi recapiti (è consigliato indicare anche il nominativo, ma non è obbligatorio) devono essere ampliamente pubblicizzati.

2.5 Destinatario

Il GPDR all'art. 4 definisce destinatario "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi". Pertanto debbono essere considerati destinatari tutti i soggetti che ricevono dati personali da un titolare, sia che siano interni o esterni, sia che li ricevono per eseguire trattamenti per conto del titolare sia che li ricevono per conseguire proprie finalità. I destinatari o le categorie di destinatari ai quali verranno comunicati i dati devono essere definiti in fase di raccolta dei dati per inserirli nell'informativa all'interessato. Nel caso che il destinatario sia un soggetto che risiede in un paese non membro dell'Unione, è richiesto che il Titolare verifichi che le garanzie offerte da questi per la protezione dei dati siano adeguate.

Soggetto del trattamento	Destinatario
Persona giuridica/fisica	Soggetto interno/esterno, persona fisica, persona giuridica
Carica/persona fisica	Rappresentante legale, persona fisica
Descrizione	Il destinatario (recipient) è il soggetto al quale sono comunicati i dati personali da parte di un titolare. Nel GDPR il "destinatario" è definito al punto 9) dell'art. 4 dove si precisa anche che può trattarsi di soggetto terzo o no (la definizione di "terzo" è riportata nel successivo punto 10) dello stesso art. 4). Devono pertanto considerarsi destinatari anche coloro che trattano i dati su "istruzioni" del titolare all'interno.
Informazioni per l'interessato	Nell'informativa da fornire all'interessato devono essere indicati i destinatari o le categorie di destinatari ai quali saranno comunicati i dati, dovranno essere elencati anche le strutture interne o le categorie di personale che verranno a conoscenza dei dati personali nello svolgimento della loro attività lavorativa.
Note	Nel caso il destinatario sia un soggetto "terzo" che riceve i dati per perseguire proprie finalità, diventerà a sua volta titolare. Il destinatario che riceve i dati da altro titolare per perseguire finalità proprie è tenuto a dare l'informativa all'interessato nel più breve tempo possibile, sempre che

	ciò non sia impossibile o richieda uno sforzo sproporzionato o se l'interessato dispone già dell'informazione o nel caso in cui la comunicazione sia necessaria per adempiere a un obbligo di legge.

2.6 Interessato

L'interessato è la persona fisica alla quale si riferiscono i dati trattati. È sempre una persona fisica. L'interessato è quindi il soggetto "proprietario" dei dati personali e su questi conserva dei diritti nei confronti del titolare del trattamento. Il GDPR al Capo III elenca nel dettaglio tali diritti. Alcuni di questi, a seconda della finalità per la quale i dati sono stati raccolti, potrebbero non essere esercitabili dagli interessati. Per esempio non è possibile effettuare la cancellazione dei dati relativi alla carriera di un lavoratore, mentre può essere accolta la richiesta di cancellazione dei recapiti personali. La risposta alle richieste dell'interessato deve comunque essere tempestiva e, anche nel caso non sia possibile soddisfarla, occorre specificare la motivazione del rifiuto. Il titolare ha il compito di facilitare l'accesso all'interessato ai suoi dati, predisponendo dei canali di comunicazione dedicati, quali ad esempio i recapiti del Responsabile della Protezione dei Dati. Per la descrizione dei trattamenti si usa raggruppare gli interessati in categorie omogenee a seconda del tipo di rapporto che questi hanno con il titolare. In ambito interno si possono individuare le seguenti principali categorie d'interessati, le quali possono poi essere suddivise in sottocategorie per distinguerle all'interno di alcuni trattamenti(clienti,fornitori,dipendenti).

2.7 L'Azienda quale Responsabile del trattamento dati

L'Azienda stipula contratti o convenzioni con soggetti esterni, nei quali si prevede l'affidamento di compiti specifici per i quali è previsto un trattamento di dati personali per finalità proprie di un soggetto affidatario (che risulta essere Titolare degli stessi). In tali casi l'organizzazione sarà designata da tale Titolare quale Responsabile del trattamento dati. In questi casi sarà necessario prevedere l'individuazione del responsabile interno che dovrà prevedere le misure di protezione adeguate e mantenere i rapporti con il Titolare per gli adempimenti richiesti.

2.8 Autorità di controllo

Le autorità di controllo sono incaricate di "sorvegliare l'applicazione del presente regolamento (GRPD) al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione" (punto 1) art. 51 del GPDR). Ogni stato membro istituisce una o più autorità pubbliche indipendenti. Nel caso siano più di una deve essere designata quella che le rappresenterà nel Comitato europeo per la protezione dei dati, che ha funzioni di coordinamento delle varie autorità di controllo, per rendere coerenti e in linea con il GDPR le varie decisioni che a queste competono. Il Comitato ha inoltre funzioni di supporto per la Commissione europea. All'Autorità di controllo nazionale devono essere comunicati eventuali data breach. Le Autorità di controllo sono competenti ad accogliere e decidere su eventuali reclami presentati dagli interessati.

3. Mappa dei trattamenti dei dati personali

3.1 Premesse inerenti i trattamenti di dati personali

Nel presente capitolo si è stilata una mappatura dei principali trattamenti che trovano svolgimento in ambito aziendale con l'obiettivo di:

1) Consentire di completare in modo più agevole il registro dei trattamenti, tenuto conto del fatto che gran parte dei dati personali e delle finalità del trattamento,

2) Individuare le informazioni che dovranno essere comunicate all'interessato, con particolare riferimento agli aspetti introdotti nel nuovo GDPR (es: indicazioni sui tempi di conservazione dei dati, finalità indicate in modo specifico), condividendo ove possibile alcune bozze di informative,
3) Mettere in evidenza alcune peculiarità del trattamento dei dati preso in esame ed eventuali considerazioni fatte in merito ai principali dubbi interpretativi.

Si è proceduto prendendo in considerazione la categoria di interessati cui il trattamento è rivolto (dipendenti – trattamenti trasversali a più categorie di interessati), per poi dettagliare i singoli trattamenti in relazione alle finalità da perseguire. Infine, per ciascuna categoria di interessati e nell'ambito delle differenti finalità perseguite, sono presi in analisi i seguenti aspetti:

	Elementi considerati
Natura dei dati	L'analisi sulla natura dei dati consente di determinare se, e in quale misura, possono essere trattati (come ad esempio: categorie particolari di dati personali di cui all''art. 9 e/o i dati relativi a condanne penali e reati di cui all'art. 10), evidenziando eventuali accorgimenti adottati nel trattamento di tali dati.
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	L'analisi sui tipi di dati che sono strettamente necessari per perseguire un obbligo legale o di quelli strettamente connessi all'esecuzione di compiti istituzionali favorisce la definizione di tempi di conservazione differenti o la previsione di differenti garanzie per l'interessato.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Tenuto conto del nuovo GDPR, nonché dell'obbligo di indicare nell'informativa "la base giuridica del trattamento" e "i legittimi interessi perseguiti dal titolare del trattamento" si ritiene opportuno fornire all'interessato maggiori dettagli sulle finalità. Sono quindi condivise anche alcune valutazioni in merito all'opportunità di raccogliere un consenso ad hoc per le diverse finalità non connesse a obblighi legali o allo svolgimento di compiti.
Note sui diritti dell'interessato	Si è ritenuto opportuno esplicitare in questa sezione alcune note inerenti i diritti dell'interessato.

Comunicazione e trasferimento all'estero	Occorre chiarire nell'informativa l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale. Tale dato è rilevante anche nell'ambito della redazione del registro, pertanto, si è ritenuto opportuno effettuare alcune note e approfondimenti su tale aspetto.
Categorie di interessati	Le categorie di persone fisiche cui si riferiscono i dati personali.
Categorie di destinatari	È previsto individuare nell'informativa le categorie di destinatari a cui i dati personali possono essere comunicati. Si dovrà quindi dare indicazione di tutte le persone che possono ricevere comunicazione di dati personali (es: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che possono venire a conoscenza dei dati, nonché, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali). Nelle schede di trattamento sotto riportate, non sono stati indicati eventuali soggetti esterni che potrebbero trattare i dati in qualità, ad esempio, di amministratori di sistema o di rete o di database, considerato che tale informazione è strettamente connessa all'organizzazione. In relazione ai destinatari, si specifica inoltre che, se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali, occorre chiarire - nell'informativa privacy - le possibili conseguenze della mancata comunicazione dei dati.
Archiviazione e conservazione	L'informativa sulla privacy dovrà indicare il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati nel periodo. Tale informazione è utile anche nell'ambito della redazione dei registri di trattamento: sarà infatti importante determinare i termini ultimi previsti per la cancellazione delle diverse categorie di dati. I trattamenti possono essere compiuti con o senza l'ausilio di processi automatizzati.

3.2 Trattamenti principali inerenti ai clienti

Sono indicati in questo paragrafo i principali trattamento di dati personali che riguardano le seguenti categorie di interessati: coloro che intendono usufruire dei prodotti e servizi.

3.2.1 Trattamento finalizzato alle scelte commerciali

	Elementi considerati
Descrizione trattamento	Il dato è trattato per favorire azioni di accompagnamento e monitoraggio atte a prevenire i comportamenti dei clienti. I dati sono trattati, ad esempio, nell'ambito di attività di: ▪ Iscrizione e acquisti ▪ Partecipazione a simulazioni di test o a colloqui individuali ▪ Invio di notifiche agli interessati o nuovi prodotti ▪ Miglioramento di attività, anche tramite percorsi personalizzati
Natura dei dati	Personali, categorie particolari di dati personali, Dati comuni di interessati che possono essere: ▪ Persone che decidono volontariamente di aderire ad attività di vendita e che in casi particolari possono essere anche minorenni ▪ Referenti presenti nei reparti/uffici.
Quali sono i dati personali Necessari per perseguire la finalità descritta	I dati personali strettamente necessari per perseguire la finalità descritta sono: dati anagrafici, dati di contatto, ente di riferimento, aree di interesse, ecc.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Il conferimento pur essendo facoltativo è necessario perché strettamente connesso allo svolgimento di attività. È consigliato tuttavia chiarire in modo specifico le differenti finalità nell'informativa per le quali si intende trattare il dato.
Archiviazione e conservazione	Considerato che il dato potrebbe essere utilizzato per favorire l'analisi della qualità delle attività (confrontando i dati raccolti, effettuando delle elaborazioni e raffronto di dati e/o verificare il successo di azioni correttive) i dati potrebbero essere archiviati e mantenuti in coerenza con il consenso acquisito per un periodo massimo di 15 anni. Tale periodo è valutato sulla base del termine massimo di durata di un percorso aziendale riferito a un singolo interessato.
Note sui diritti dell'interessato	Non è consentita la rettifica dei risultati previsti.
Categorie di interessati	--

Categorie di destinatari	Commerciali
Comunicazione e trasferimento all'estero	I dati non sono comunicati all'estero.

3.3 Trattamenti principali inerenti a dipendenti e/o collaboratori

Sono indicati in questo paragrafo i principali trattamento di dati personali che riguardano:

- il personale dipendente e/o i collaboratori
- soggetti terzi (esempio: fornitori, clienti, ecc.).

3.4 Trattamento finalizzato alla gestione del rapporto di lavoro

	Elementi considerati
Descrizione del trattamento	Trattamento necessario per la gestione del rapporto di lavoro o di collaborazione, anche per personale in convenzione. In questo trattamento rientrano anche la: ▪ gestione dell'offerta formativa e dell'assegnazione degli incarichi ▪ gestione della struttura organizzativa, dell'anagrafica del personale e registrazione degli eventi ▪ gestione delle pratiche assicurative e previdenziali; trattamenti assistenziali; denunce e pratiche di infortunio, trattamenti assistenziali ▪ trattamento dei dati inerenti i procedimenti disciplinari a carico del personale e nei giudizi pendenti di fronte a tutte le giurisdizioni che coinvolgono dipendenti, collaboratori ▪ gestione delle risorse umane (posizioni organizzative, profili di competenza, repertorio aziendale delle conoscenze, processo di selezione, politiche retributive) ▪ gestione della formazione ▪ rilevazione e gestione delle presenze ▪ gestione retributiva ▪ gestione dei provvedimenti per il personale (es. m trasferimenti, ecc.) ▪ programmazione annuale degli obiettivi, finalizzata alla valutazione del personale, alla pianificazione finanziaria e alla predisposizione del budget.
Natura dei dati	Personali, categorie particolari di dati personali, dati personali relativi a condanne penali e reati.
Quali sono i dati personali strettamente necessari per perseguire la finalità	Il principio di minimizzazione impone una selezione dei dati da trattare in relazione allo specifico servizio o finalità perseguita, ad esempio: ▪ per la gestione dei dati anagrafici e amministrativo contabili dei collaboratori esterni possono essere trattati dati inerenti l'anagrafica, dati bancari, fiscali e previdenziali;

descritta	▪ per la gestione del personale docente possono essere trattati dati relativi alla costituzione/cessazione del rapporto di lavoro, alle procedure di valutazione comparativa, al reclutamento, agli affidamenti, agli incarichi esterni; ▪ per la gestione personale possono essere trattati dati relativi alla costituzione/cessazione del rapporto di lavoro, a concorsi e selezioni, a incarichi esterni, alla mobilità. ▪ per la gestione degli istituti contrattuali possono essere trattati dati relativi a congedi, permessi, aspettative, malattie, infortuni, partecipazioni a scioperi e assemblee, ecc.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa al momento dell'assunzione e dell'avvio del rapporto di collaborazione.
Archiviazione e conservazione	Rispetto ai tempi di archiviazione/conservazione si specifica quanto segue: 1) L'anagrafica e i dati di carriera sono conservati illimitatamente nel tempo. 2) I dati inerenti graduatorie o verbali sono conservati illimitatamente nel tempo. 3) La conservazione dei restanti dati è sotteso ai tempi di conservazione degli atti amministrativi che li contengono
Note sui diritti dell'interessato	In merito alla cancellazione dei dati – non può essere concessa la cancellazione di dati personali che, per la normativa vigente o in ragione di regole previste nei massimari o nei regolamenti interni devono essere conservati illimitatamente nel tempo.
Categorie interessati	Tutti i dipendenti dell'organizzazione e collaboratori.

Categorie destinatari	Ufficio Personale Altri soggetti pubblici o privati, tra cui: ▪ Amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000; ▪ INPDAP – INPS (per erogazione e liquidazione trattamento di pensione, L. 335/1995; L. 152/1968); ▪ Comitato di verifica per le cause di servizio e Commissione medica territorialmente competente (nell'ambito della procedura per il riconoscimento della causa di servizio/equo indennizzo, ai sensi del DPR 461/2001); ▪ INAIL, Autorità di P.S., Sportello unico per l'immigrazione (DPR n. 334/2004) e/o altre Autorità previste dalla legge (per denuncia infortunio, DPR 1124/1965); ▪ Strutture sanitarie competenti (per visite fiscali, art. 21 CCNL del 06/07/1995, CCNL di comparto); ▪ Soggetti pubblici e privati ai quali, ai sensi delle leggi regionali/provinciali, viene affidato il servizio di formazione del personale; ▪ Direzione Territoriale del lavoro (per le aspettative e per i casi di contenzioso) ▪ Centro per l'impiego o organismo territorialmente competente per le assunzioni ai sensi della legge 68/1999; ▪ Amministrazioni provinciali e Centro regionale per l'impiego in ordine al prospetto informativo delle assunzioni, cessazioni e modifiche al rapporto di lavoro, redatto ai sensi della L. 68/1999; ▪ Autorità giudiziaria (C.P. e C.P.P.); ▪ Organizzazioni sindacali per gli adempimenti connessi al versamento delle quote di iscrizione e per la gestione dei permessi sindacali; ▪ Ministero delle Finanze, nell'ambito dello svolgimento da parte delle Azienda del ruolo di Centro di assistenza fiscale (CAF), relativamente alla dichiarazione dei redditi dei dipendenti (art.17 D.M. 164/1999 e art. 2-bis D.P.R. 600/1973); ▪ Pubbliche Amministrazioni presso le quali vengono comandati i dipendenti, nell'ambito della mobilità dei lavoratori.
Comunicazione trasferimento all'estero	I dati non possono essere trasferiti all'estero.

ECA

3.5. Trattamento di dati personali ai fini di formazione e aggiornamento professionale

	Elementi considerati
Descrizione del trattamento	Il trattamento di dati personali è svolto per l'erogazione di attività didattiche e di formazione (frontale, multimediale e a distanza). Rientrano in questo tipo di trattamento anche i trattamenti per: ▪ Iscrizione a corsi di formazione ▪ Gestione dei registri delle attività didattiche: consuntivazione attività didattiche e non, a preventivo e consuntivo ▪ Valutazioni qualità, nell'ipotesi in cui i questionari possano essere indirettamente riconducibili a un interessato. ▪ Eventuali attestati di frequenza ai corsi
Natura dei dati	Personali, categorie particolari di dati personali
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	In relazione allo specifico servizio erogato, potrebbero essere trattati: dati presenti in anagrafica, dati di carriera, curriculum vitae, ore di rendicontazione, iscrizioni e partecipazioni a corsi di formazione.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	L'informativa potrebbe essere inclusa tra le informazioni rese al momento della gestione del rapporto di dipendenza o collaborazione. Nel caso in cui, durante la sessione di formazione, siano registrate le immagini e/o le voci dei partecipanti, si rende opportuno informare gli interessati di tale trattamento mediante, ad esempio, affissione dei cartelli informativi
Archiviazione e conservazione	Gli atti connessi alle attività di formazione svolte dai partecipanti potrebbero avere un tempo di conservazione. La conservazione delle registrazioni audio/video dovrà essere stabilita nell'informativa in relazione alle specifiche finalità perseguite dall'ente.
Note sui diritti dell'interessato	Potrebbe essere garantita l'opposizione a specifiche operazioni di trattamento delle riprese audio-video (es: nel caso di diffusione del video su internet).
Categorie di destinatari	Strutture deputate alla formazione e all'aggiornamento professionale di dipendenti e collaboratori (ad esempio nell'ambito di corsi di formazione erogati tra più azienda partner). Enti esterni eroganti il servizio di formazione e aggiornamento professionale.
Comunicazione e trasferimento all'estero	Non previsti.
Categorie interessati	Personali

ECA

3.6. Trattamento necessario per politiche Welfare e per la fruizione di agevolazioni

	Elementi considerati
Descrizione del trattamento	Il dato è trattato al fine di consentire la promozione di politiche volte a consentire al personale dell'Azienda di fruire di agevolazioni, servizi e/o sussidi.
Natura dei dati	Personali, categorie particolari di dati personali (disabilità, ecc).
Dati personali strettamente necessari per perseguire la finalità descritta	Anagrafica (eventualmente anche dati familiari), carriera e dati, ISEE. Potrebbero rendersi necessari altri dati connessi al tipo di servizio.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa al momento dell'assunzione.
Archiviazione e conservazione	Basato prevalentemente su obblighi di legge e regolamenti.
Note sui diritti dell'interessato	-
Categorie di interessati	Dipendenti e familiari.
Categorie di destinatari	Fornitori/Enti/Cooperative ad es. per attività dopo Lavoro, Aziende per erogazione polizze assicurative per il personale Enti esterni per realizzare servizi integrati a favore dei dipendenti e/o preposti a favorire l'attuazione di politiche Welfare
Comunicazione e trasferimento all'estero	I dati non sono comunicati all'estero.

ECA

3.7. Trattamenti effettuati dal Medico Competente

	Elementi considerati
Descrizione del trattamento	Il dato è trattato dal Medico Competente al fine di svolgere l'attività di sorveglianza sanitaria obbligatoria del personale, ottemperando agli obblighi di legge come definiti dal D. Lgs. 81/08 - Testo Unico in materia di salute e sicurezza del lavoro
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Informativa specifica per il servizio da rendere all'interessato all'atto della visita medica
Archiviazione e conservazione	I tempi di conservazione dei dati sono strettamente dipendenti dagli ambiti di gestione (es: fascicolo sanitario/referti/gestione amministrativa) e dalle norme vigenti in tali ambiti
Note sui diritti dell'interessato	-
Categorie di interessati	Tutti i dipendenti dell'organizzazione e collaboratori sulla base dei protocolli di rischio in rapporto alle attività svolte
Categorie di destinatari	Ufficio Prevenzione, Protezione e Sicurezza; Ufficio Personale.
Comunicazione e trasferimento all'estero	I dati non vengono comunicati all'estero, salvo casi specifici che lo richiedano (es. emergenze sanitarie)
Natura dei dati	Personali, categorie particolari di dati personali (dati inerenti lo stato di salute, referti medici)
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici, dati di contatto, dati inerenti lo stato di salute, dati inerenti l'attività lavorativa svolta e di carriera

3.8.Trattamenti effettuati dall'Ufficio Prevenzione, Protezione e Sicurezza

	Elementi considerati
Descrizione del trattamento	Il dato è trattato dall'Ufficio Prevenzione, Protezione e Sicurezza al fine di supportare il Medico Competente nell'attività di sorveglianza sanitaria obbligatoria del personale, ottemperando agli obblighi di legge come definiti dal D. Lgs. 81/08 - Testo Unico in materia di salute e sicurezza del lavoro.
Natura dei dati	Personali, categorie particolari di dati personali (dati inerenti lo stato di salute).
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici, dati di contatto, dati inerenti lo stato di salute, dati inerenti l'attività lavorativa svolta e di carriera.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa al momento dell'assunzione.
Archiviazione e conservazione	I tempi di conservazione dei dati sono strettamente dipendenti dagli ambiti di gestione e dalle norme vigenti in tali ambiti.
Categorie di interessati	Tutti i dipendenti dell'organizzazione e collaboratori sulla base dei protocolli di rischio in rapporto alle attività svolte.
Categorie di destinatari	Ufficio Personale; Medico Competente.
Comunicazione e trasferimento all'estero	I dati non possono essere comunicati all'estero.
Note sui diritti dell'interessato	-

3.9. Trattamento dei dati personali nell'ambito dell'erogazione del servizio di telefonia fissa e mobile

	Elementi considerati
Descrizione del trattamento	Il dato è trattato al fine di gestire tutte le attività inerenti la gestione delle linee telefoniche fisse e/o mobili e dei dispositivi, la relativa rendicontazione, nonché il servizio di assistenza.
Natura dei dati	Personali.
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Anagrafica del personale, carriera, struttura di afferenza, prefissi, chiamate da/all'esterno, spese, abilitazioni alla doppia fatturazione, altre informazioni sul traffico dati, quali: a. il numero o l'identificazione dell'utente e del soggetto cui la chiamata è trasmessa; b. il numero totale degli scatti o il tempo di durata del traffico da considerare per il periodo di rendicontazione; c. il tipo, l'ora di inizio e la durata delle chiamate effettuate e il volume dei dati trasmessi; d. la data della chiamata o dell'utilizzazione del servizio; e. informazioni concernenti i pagamenti. Con riguardo alla telefonia mobile, verranno trattati anche ulteriori dati personali con finalità di rendicontazione ed addebito.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Con riferimento alla telefonia fissa, le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa al momento dell'assunzione. In relazione alla telefonia mobile, è opportuno rilasciare apposita informativa all'atto della consegna del telefono di servizio.
Archiviazione e conservazione	6 mesi per i dati di traffico telefonico (nel caso di dati non tracciati dall'operatore telefonico).I tempi di conservazione dei dati di traffico telefonico tracciati dall'operatore sono quelli stabiliti dalla normativa vigente.
Categorie di interessati	Tutti gli intestatari di un'utenza fissa e/o mobile; soggetti che ricevono o effettuano delle chiamate su utenze.
Categorie di destinatari	I responsabili delle strutture per le utenze di competenza; i soggetti che gestiscono la fatturazione nelle singole strutture; la struttura che si occupa della gestione dei servizi di telefonia.
Comunicazione e trasferimento all'estero	I dati non vengono comunicati all'estero.
Note sui diritti dell'interessato	-

3.10 Trattamenti trasversali o connessi ad attività trasversali

	Elementi considerati
Descrizione del trattamento	Il dato è trattato al fine di permettere l'utilizzo degli spazi, per attività quali: ▪ assegnazione degli spazi alle strutture, allocazione delle persone negli spazi; ▪ controllo accessi da parte di: dipendenti, collaboratori.
Natura dei dati	Personali, categorie particolari di dati personali (dati inerenti lo stato di salute).
Archiviazione e conservazione	I tempi di conservazione dei dati personali sono legati alle procedure interne di gestione degli spazi. Nel caso in cui siano affidati spazi a soggetti esterni la conservazione dei dati sarà strettamente connessa ai tempi di conservazioni previsti dalle norme vigenti in materia contabile.
Note sui diritti dell'interessato	-
Categorie di interessati	Tutti i dipendenti, collaboratori e soggetti terzi.
Categorie di destinatari	Strutture preposte alla gestione logistica, responsabili di struttura ed eventuali soggetti delegati alla gestione della logistica.
Comunicazione e trasferimento all'estero	-
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Con riferimento al richiedente lo spazio, verranno trattati dati di anagrafica personale e di carriera. In relazione all'utilizzo degli spazi da parte di soggetti terzi, verranno trattati anche ulteriori dati personali, riconducibili ad esigenze di carattere amministrativo. Per l'accesso agli spazi da parte di soggetti disabili, potranno esser trattati dati inerenti lo stato di salute. L'eventuale decisione di effettuare il controllo degli accessi potrebbe comportare la raccolta di dati di ingresso/uscita/identificativo utente (ad es. il badge).
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Con riferimento a soggetti interni all'ente, le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa al momento dell'attivazione del rapporto con l'Azienda. Nel caso di soggetti terzi, dovrà essere rilasciata apposita informativa all'atto del conferimento dei dati.

3.11 Trattamento dei dati personali per la gestione delle postazioni

	Elementi considerati
Descrizione del trattamento	Il dato è trattato per garantire il corretto funzionamento di postazioni di lavoro fisse / mobili assegnate agli utenti, la sicurezza delle stesse e per fornire il necessario supporto nell'utilizzo.
Natura dei dati	Qualsiasi tipologia di dato utilizzato dall'utente
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati relativi all'utente, struttura di afferenza, dati di contatto. Associazione utenti/postazioni assegnate. Nella gestione delle postazioni, in dipendenza del tipo di intervento, potrebbero verificarsi da parte degli amministratori di sistema accessi, anche fortuiti, a categorie particolari di dati personali memorizzati sulle postazioni, in ragione dell'effettiva capacità di azione sulle informazioni e della rilevanza e specificità del ruolo.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa al momento dell'attivazione del rapporto (assunzione, attivazione del contratto di collaborazione).
Note sui diritti dell'interessato	Anche in relazione alla tipologia di monitoraggio effettuato e ai software utilizzati, nell'eventualità in cui possa derivarne un controllo a distanza del lavoratore, occorrerà verificare la necessità di stipulare un accordo con le rappresentanze sindacali o con la sede territoriale competente dell'Ispettorato nazionale del lavoro. Al contrario, l'installazione e utilizzo di software per garantire il monitoraggio, la sicurezza e la gestione delle postazioni saranno possibili se strettamente connessi al rapporto di lavoro.
Categorie di interessati	Tutti gli utilizzatori di postazioni soggette ad autenticazione.
Categorie di destinatari	Gestore delle postazioni e dell'assistenza.
Comunicazione e trasferimento all'estero	Eventuale produttore di soluzioni SW installate (S.O., applicativi, endpoint security)
Archiviazione e conservazione	I tempi di conservazione dei dati personali relativi alle assegnazioni ed ai ticket di segnalazioni sono legati alle procedure interne di gestione. I tempi di conservazione di altre informazioni personali variano in funzione del tipo di intervento effettuato.

3.12 Trattamento per la gestione degli infortuni

	Elementi considerati
Descrizione del trattamento	Il trattamento viene effettuato in relazione agli infortuni occorsi al personale ed ai soggetti terzi in visita. In particolare nell'ambito della gestione di tali eventi da parte degli uffici dell'Azienda preposti, dalla presa in carico della segnalazione di infortunio fino alla chiusura della relativa pratica, includendo: - l'interazione con enti esterni - la gestione di eventuali prescrizioni da parte dell'INAIL - l'apertura e gestione della segnalazione di sinistro nell'ambito di copertura delle polizze assicurative dell'Azienda - la valutazione delle proposte di liquidazione del danno - gli eventuali prolungamenti del periodo di infortunio
Natura dei dati	Personali, categorie particolari di dati personali (dati inerenti lo stato di salute).
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici, di carriera e dati inerenti lo stato di salute. Dati specifici relativi all'infortunio occorso (es referti, certificati).
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti all'atto dell'apertura del sinistro.
Archiviazione e conservazione	Il tempo di conservazione dei dati dipende dallo specifico procedimento e si basa su quanto previsto da obblighi di legge o regolamenti interni.
Note sui diritti dell'interessato	-
Categorie di interessati	Tutto il personale dell'organizzazione e soggetti terzi.
Categorie di destinatari	Uffici dell'Azienda coinvolti nella gestione degli infortuni, broker, compagnia assicuratrice, Inail, eventuali ulteriori enti coinvolti.
Comunicazione e trasferimento all'estero	I dati non saranno comunicati all'estero.

3.13 Trattamento finalizzato alla Conservazione Documentale

	Elementi considerati
Descrizione del trattamento	Gestione delle attività di conservazione documentale ai sensi della normativa vigente.
Natura dei dati	Ogni dato e documento inserito nel sistema di protocollo informatico e potenziale oggetto di invio in conservazione, ovvero: - descrizione del documento e sua rappresentazione, ovvero numero di protocollo ed eventuale repertorio, data, oggetto, allegati, classificazione, file associati - indicazione dei corrispondenti/contraenti e dei responsabili e assegnatari del documento In funzione del procedimento/attività i documenti possono contenere dati personali, anche appartenenti a particolari categorie.
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Dati anagrafici dei mittenti e destinatari. Il campo oggetto, incluso nel nucleo minimo delle informazioni necessarie per la registrazione a protocollo, potrebbe per sua natura riportare dati personali, anche appartenenti a particolari categorie (es sensibili o giudiziari). I dati trattati dipendono dallo specifico procedimento/affare/attività e sempre nell'osservanza del DPCM 3.12.2013, tanto in materia di protocollo informatico (ai sensi degli articoli 40bis, 41, 47, 57bis e 71 del CAD) tanto in materia di conservazione (ai sensi degli articoli 20, commi 3 e 5bis, 23ter, comma 3, 43, commi 1 e 3, 44, 44bis e 71 comma 1 del CAD) Potrebbe rendersi necessaria anche la registrazione di ulteriori dati personali per supportare e motivare: - la creazione del pacchetto di distribuzione per motivi legali; - l'accesso al sistema di conservazione per la verifica dell'operato del conservatore o per verifiche di carattere tecnico.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa al momento dell'assunzione, per il personale.
Note sui diritti dell'interessato	-
Categorie interessati	personale, terzi.
Categorie destinatari	- Reparti aziendali – e loro operatori e delegati - preposte a processo di gestione documentale e alla conservazione. - Destinatari del pacchetto di distribuzione per motivi legali o accesso agli atti previa autorizzazione della struttura organizzativa coinvolta.
Comunicazione trasferimento all'estero	-

ECA

Archiviazione e conservazione	Il tempo di conservazione dei dati dipende dallo specifico procedimento/affare/attività e si basa su quanto previsto da obblighi di legge e da regolamenti interni. Per quanto attiene la conservazione illimitata, si ricordano le principali tipologie di documentazione: Verbali e Delibere, Contratti, gare e convenzioni. Per quanto riguarda le fatture e i documenti contabili la conservazione è 10 anni. In materia di conservazione accreditata, ogni accordo di versamento prevede specifico riferimento al tempo di conservazione (illimitato, limitato).

3.14 Trattamento finalizzato all'acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso

	Elementi considerati
Descrizione del trattamento	Il dato è trattato per consentire la verifica di posizioni giudiziarie, fiscali e di condotta di fornitori ed operatori economici che sono in rapporto con l'organizzazione al fine di: ▪ svolgere le attività preliminari connesse alle procedure di acquisizione di beni e servizi; ▪ coordinare e analizzare la redazione della documentazione tecnica, amministrativa e contrattuale; ▪ gestire il procedimento e le attività connesse (stipula del contratto, monitoraggio dei tempi del procedimento in affidamento).
Natura dei dati	Personali, dati personali relativi a condanne penali e reati
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Potrebbe rendersi necessaria la registrazione di dati personali presenti nella documentazione inerente: ▪ DURC (acquisendo parte dei dati da Inps e altri da Inail) ▪ Visure camerali ▪ Certificato di Casellario Giudiziale (Tribunale) ▪ accertamenti sulla situazione societaria e personale delle controparti (Anac) ▪ verifica regolarità fiscale (Agenzia delle entrate ed Equitalia per il pregresso) Nel caso di acquisti sopra soglia è necessario altresì acquisire i dati inerenti: Offerta economica, certificazioni antimafia.

ECA

Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	L'informativa può essere resa al momento della pubblicazione del bando per la fornitura di beni o servizi. Al momento della stipula del contratto si può consegnare un'ulteriore informativa più specifica in funzione del servizio reso o del bene acquisito.
Archiviazione e conservazione (tempi, modi, quali dati)	I tempi possono essere molto diversi a seconda del tipo di contratto e dell'oggetto della fornitura. Il criterio per stabilirli si basa su principi di buon senso e sulle precisazioni dell'Autorità Garante secondo cui i dati possono essere conservati in generale "finché sussista un interesse giustificabile" e cioè finché la loro conservazione risulti necessaria agli scopi per i quali sono stati raccolti e trattati. Ad esempio nel caso in cui si acquisti un bene con garanzia a vita o un software con licenza d'uso illimitata in senso temporale i dati possono essere conservati a tempo indeterminato, comunque fino a che il bene o il software non viene dismesso. Più in generale, i dati dovrebbero essere conservati in linea con quanto previsto dal Codice Civile (art. 2220).
Note sui diritti dell'interessato	-
Categorie interessati	Fornitori di beni e servizi, operatori economici.
Categorie destinatari	Strutture preposte all'acquisto di beni e servizi, alla liquidazione o alla gestione del contenzioso; struttura preposta al rispetto delle norme su trasparenza e anticorruzione.
Comunicazione trasferimento all'estero	-

3.15 Trattamento finalizzato alle verifiche sull'espletamento di lavori, in cantiere

	Elementi considerati
Descrizione trattamento	Il dato è trattato per la valutazione amministrativa ed economica di terzi, fornitori per l'espletamento di lavori in appalto, verifiche sui cantieri o presso installazioni.
Natura dei dati	Personali, categorie particolari di dati personali, dati personali relativi a condanne penali e reati.
Archiviazione e conservazione	I tempi di conservazione dei dati dipendono dallo specifico procedimento e dalla normativa vigente in materia di appalti, sicurezza sul lavoro e conduzione di cantieri.
Note sui diritti dell'interessato	-
Categorie di interessati	Fornitori.
Categorie di destinatari	Uffici Acquisto
Comunicazione e trasferimento all'estero	Normalmente non ci sono comunicazioni all'esterno.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	L'informativa è predisposta al momento del contratto.
Quali sono personali strettamente necessari	Potrebbe rendersi necessaria la registrazione di dati personali per consentire, ad esempio: 1) La consultazione del contratto dei lavoratori delle ditte appaltatrici e di quelle sub-appaltate.

3.16 Trattamento finalizzato alla gestione del contenzioso e del recupero crediti

	Elementi considerati
Descrizione del trattamento	Il dato è trattato per: ▪ la gestione dei contenziosi instaurati avanti le diverse autorità giudiziarie in cui sia coinvolta l'organizzazione; ▪ l'attività di recupero dei crediti dell'organizzazione nei confronti di personale e di soggetti terzi inadempienti.
Natura dei dati	Personali, categorie particolari di dati personali, dati personali relativi a condanne penali e reati.
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	I dati trattati possono essere differenti a seconda del tipo di contenzioso; includerà in ogni caso i dati anagrafici e il tipo di rapporto potrebbe includere dati sanitari. Per il recupero crediti, la tipologia di dati trattati sarà in correlazione alla categoria di interessati coinvolta.
Archiviazione e conservazione (tempi, modi, quali dati)	I tempi di conservazione sono definiti per legge.
Note sui diritti dell'interessato	-
Categorie di interessati	Sono interessati potenzialmente tutti i soggetti che abbiano un rapporto con l'Azienda: personale, candidati, soggetti terzi (fornitori). Può interessare anche persone che non hanno rapporti di alcun tipo con l'Azienda. Con riguardo ad alcuni contenziosi e procedimenti di recupero crediti potrebbero essere interessati anche i familiari dei soggetti direttamente coinvolti.
Categorie di destinatari	Ufficio preposto, Avvocatura dello Stato (quando rappresenta l'Azienda in giudizio), Autorità Giudiziarie e Agenzia delle Entrate (nel caso di iscrizione a ruolo dei crediti).
Comunicazione e trasferimento all'estero	Potrebbe esser necessaria la comunicazione e/o il trasferimento di dati all'estero nei casi di contenzioso con soggetti esteri e nel caso di recupero crediti da debitori esteri, con affidamento della pratica a professionisti stabiliti nei paesi dei soggetti con i quali si sia instaurata la lite.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità potrebbero essere inserite in un'apposita informativa o nell'informativa generale resa: ▪ al personale lavoratore; ▪ a soggetti terzi e aziende fornitrici di beni e servizi.

ECA

3.17 Trattamento di dati nell'ambito dei servizi di posta elettronica

	Elementi considerati
Descrizione del trattamento	Al fine di favorire la collaborazione, l'organizzazione potrebbe fornire strumenti informatici (es: web conference, spazi virtuali di collaborazione, ecc) tramite i quali possono essere trattati dati personali funzionali: ▪ all'erogazione del servizio stesso ▪ a connesse attività di risoluzione dei guasti ▪ alla valutazione dell'uso del servizio e della qualità (es: mediante rilevazioni statistiche basate sull'uso di tali strumenti) ▪ a garantire la sicurezza informativa dei dati trattati mediante tali strumenti di collaborazione.
Natura dei dati	Personali, categorie particolari di dati personali.
strettamente necessari per perseguire la finalità descritta	elettronica, l'indirizzo IP del sistema utilizzato, dati relativi alla carriera, dati anagrafici, ecc.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	L'informativa dovrebbe essere resa prima dell'accesso al sistema, qualora non specificato in informative specifiche.
Archiviazione e conservazione	I tempi possono essere molto diversi a seconda del tipo di strumento utilizzato e della finalità perseguita. Il criterio per stabilirli si basa su principi di buon senso e sulle precisazioni dell'Autorità Garante secondo cui i dati possono essere conservati in generale "finché sussista un interesse giustificabile" e cioè finché la loro conservazione risulti necessaria agli scopi per i quali sono stati raccolti e trattati. Normalmente tale periodo di conservazione non supera i 6 mesi.
Note sui diritti dell'interessato	-
Categorie di interessati	Personale dipendente, collaboratori esterni, altri soggetti utilizzatori del servizio
Categorie di destinatari	Ufficio preposto alla gestione e/o utilizzo dello strumento di collaborazione.
Comunicazione e trasferimento all'estero	I dati non sono comunicati all'estero.
Quali sono i dati personali	A seconda del tipo di attività o strumento di collaborazione potrebbero essere utilizzati dati quali, l'indirizzo di posta

3.18 Trattamento finalizzato all'erogazione di servizi di posta elettronica

	Elementi considerati
Descrizione del trattamento	Al fine di favorire la comunicazione istituzionale tramite i servizi di posta elettronica, l'organizzazione potrebbe trattare dati personali funzionali a: ▪ l'erogazione del servizio stesso ▪ lo svolgimento attività connesse alla risoluzione dei guasti ▪ la valutazione dell'uso del servizio e della qualità dei servizio ▪ garantire la sicurezza informativa dei dati trattati
Natura dei dati	Personali.
Modalità per fornire l'informativa e, ove necessario, acquisire il consenso	Le informazioni inerenti il trattamento di dati personali per questa finalità dovrebbero essere inseriti nell'informativa generale resa all'assunzione , per il personale alla richiesta di creazione dell'account per soggetti terzi.
Archiviazione e conservazione	In generale dipende dai regolamenti interni, che spesso prevedono differenze di trattamento a seconda del tipo di utente (es. tempi di cancellazione della casella di posta diversi).
Note sui diritti dell'interessato	Cancellazione solo dopo un determinato periodo dalla cessazione del rapporto.
Categorie di interessati	Personale dipendente e non, ospiti frequentatori.
Categorie di destinatari	Struttura preposta al servizio di posta elettronica.
Comunicazione e trasferimento all'estero	Solo nel caso di servizio di posta esternalizzato su outsourcer estero.
Quali sono i dati personali strettamente necessari per perseguire la finalità descritta	Indirizzi e-mail. All'atto della creazione dell'account o in caso di cambio di status dell'utente (se sono previste differenze di gestione delle caselle a seconda del ruolo), anche anagrafica dell'utente (codice fiscale, matricola, ruolo ricoperto). Nella gestione legata al troubleshooting, incidenti di sicurezza e azioni preventive sulla diffusione di messaggi malevoli, potrebbe rendersi necessario il trattamento dei seguenti dati connessi ai messaggi di posta: casella di posta sorgente, casella destinataria, server in entrata e uscita, server di transito, oggetto mail, timestamp.

4. TRACCIAMENTO INFORMAZIONI NON PRIMARIE

Le comunicazioni elettroniche fatte nei luoghi di lavoro possono essere coperte dalle nozioni di "vita privata" e "corrispondenza" ai sensi dell'articolo 8, paragrafo 1 della Convenzione europea. Pertanto, nell'esecuzione delle attività di log e tracciamento è necessario considerare quanto stabilito sui principi fondamentali della protezione dei dati dalla direttiva UE Directive 95/46/EC (UE) e dagli ulteriori obblighi introdotti dal GDPR. A tale scopo il WP art. 29 ha recentemente espresso il suo parere sul trattamento dei dati sul posto di lavoro e sulla sorveglianza delle comunicazioni elettroniche, che integra quanto già precedentemente espresso con il 08/2001 al fine di fornire orientamenti per bilanciare le aspettative della privacy dei lavoratori (e/o collaboratori) sul posto di lavoro con il legittimo interesse del datore di lavoro. Dunque, i datori di lavoro possono raccogliere i dati ad es. di monitoraggio solo per scopi specifici e legittimi, con l'elaborazione che si svolge in condizioni adeguate (ad esempio, proporzionate e necessarie, per un interesse reale e attuale, in modo legittimo, articolato e trasparente) sulla base di un fondamento giuridico per il trattamento dei dati personali raccolti o generati tramite comunicazioni elettroniche. Poiché il consenso espresso dal lavoratore può solo raramente essere considerato libero, visto lo squilibrio di potere del datore di lavoro, allora il fondamento giuridico al monitoraggio può essere costituito dal legittimo interesse ma questo solo se l'elaborazione è strettamente necessaria per uno scopo legittimo e l'elaborazione è conforme ai principi di proporzionalità e di sussidiarietà. Perciò prima di introdurre uno strumento che può dar luogo al monitoraggio e tracciamento dei lavoratori è necessario condurre un test di proporzionalità per valutare se tutti i dati siano necessari, se questa elaborazione non contrasta con i diritti generali sulla privacy che i dipendenti hanno sul posto di lavoro e quali misure devono essere adottate per garantire che siano minimizzati al minimo le possibilità di sconfinamento nella vita privata e nel diritto alla segretezza delle comunicazioni. E' altrettanto importante adottare il principio di minimizzazione dei dati così raccolti, inoltre le informazioni (ad es. i log) devono essere memorizzate per il

periodo di tempo minimo necessario e devono essere cancellate appena non risultano più necessarie. Come esempio di buone pratiche, prima di introdurre nuovi strumenti potenzialmente intrusivi, o qualsiasi tecnologia di monitoraggio va effettuata un Data Protection Impact Assessment (DPIA). In secondo luogo, i datori di lavoro devono attuare e comunicare le Acceptable Use Policy (AUP) che descrivono l'utilizzo consentito della rete e delle attrezzature dell'organizzazione. In terzo luogo è opportuno fornire una comunicazione efficace ai dipendenti in merito a qualsiasi monitoraggio che si svolge, alle finalità di questo monitoraggio e alle circostanze, nonché alle possibilità per i dipendenti di impedire che i propri dati siano acquisiti mediante tecnologie di monitoraggio. Le politiche e le norme relative al legittimo monitoraggio devono essere chiare e facilmente accessibili. Sarà necessario valutare a seconda dei casi, se l'adozione di una certa tecnologia di monitoraggio, non richieda legalmente l'approvazione dei Sindacati o di una rappresentanza dei lavoratori. In generale alla prevenzione dovrebbe essere dato molto più peso rispetto alla rilevazione: gli interessi del datore di lavoro sono meglio serviti prevenendo l'uso abusivo degli strumenti piuttosto che l'adozione di tecnologie atte ad individuare i casi di abuso.

Finalità del tracciamento

La registrazione di eventi, caratterizzati anche dal trattamento di dati personali, effettuata su file di log o tabelle da parte di componenti sistemistiche o applicative trasversali, fa tipicamente riferimento alle seguenti finalità:

- Registrazione per adempimento di un obbligo normativo (es. leggi o regolamenti)
- Registrazione di eventi per vincoli di natura sistemistica (es. dati che per motivi di carattere tecnico sono strettamente necessari per l'erogazione di un servizio)
- Registrazione di eventi per garantire la protezione dei dati e/o dei sistemi informatici (es. per supportare attività proattive o reattive di cyber security o di protezione dei dati)
- Registrazione di eventi a supporto del troubleshooting per garantire il regolare funzionamento dei servizi informatici

- Registrazione della sequenza di eventi generati dagli utenti nell'ambito di un processo amministrativo al fine di supportare attività di ricostruzione e verifica
- Verifica del reale utilizzo di un servizio o di un suo utilizzo coerente con le finalità d'uso previste ed autorizzate.
- Rendicontazione interna per fini amministrativi (es. imputazione dei costi telefonici, di servizi di copisteria, di servizi in cloud)

Nei tempi e nei modi previsti dalla normativa, le informazioni registrate per le finalità sopra descritte possono essere oggetto di acquisizione da parte della Polizia giudiziaria per eventuali attività di indagine.

Tracciamento sistemistico e di rete

Ricadono in questo ambito i dati di tracciamento generati da apparati di rete e componenti infrastrutturali.

a. Obbligo normativo	b. Vincoli tecnologici	c. Protezione dati e	d. Troubleshooting	e. Analisi workflow	f. Verifica utilizzo	g. Rendicontazion	Ambito di servizio del trattamento
X	X	X	X				Connessione a reti autenticate (sia wifi che wired) in contesto 802.1x tramite credenziali o certificato
X	X	X	X			X	Strumenti di analisi e gestione della sicurezza di rete e dei sistemi client/server
X	X	X	X				Accesso a file server
X	X	X	X				Accesso remoto alle applicazioni
X	X	X	X		X	X	Utilizzo di pacchetti sw
X	X	X	X		X	X	Utilizzo e gestione delle postazioni gestite
	X	X	X		X	X	Utilizzo di servizi di stampa
X	X	X	X		X	X	Accesso VPN

	X	X	X	X	X	X	Gestione traffico telefonico e contabilizzazione
	X	X	X		X	X	Gestione traffico rete per videoconferenza, streaming e videosorveglianza
		X	X	X	X	X	Gestione e movimentazione linea telefonica
X	X	X	X		X	X	Accesso remoto alle postazioni utente
	X	X	X		X		Accesso a risorse (file) in Cloud
X	X	X	X		X		Accesso a risorse su directory (LDAP/AD) locali/remote
X	X	X	X		X		Accesso a sistema di autenticazione centrale
X	X	X	X		X		Gestione utenze per Identity ed Access Management
X	X	X	X		X		Gestione di servizi di proxy
X	X	X	X		X		Accesso amministrativo esterno su nostre risorse sistemistiche
X	X	X	X		X		Accesso a postazioni dei laboratori informatici
X	X	X	X		X		Accesso su dispositivi mobili
X	X	X	X		X		Gestione Sistema di Posta /Cloud
X	X	X	X		X		Accesso a macchine virtuali/servizi /Cloud

ECA

4.1 Tracciamento applicativo

Dati di sessione e di tracciamento applicativo delle attività dell'utente.

a. Obbligo normativo	b. Vincoli tecnologici	c. Protezione dati e sistemi	d. Troubleshooting	e. Analisi workflow	f. Verifica utilizzo risorsa	g. Rendicontazione	Ambito di servizio del trattamento	Informazioni tracciate
		X	X	X	X	X	Autenticazione per l'accesso alle applicazioni da client	Timestamp / Username / Servizio
		X	X	X	X	X	Utilizzo di applicazioni client sviluppate	Traccia delle attività svolte dall'utente con dettagli dipendenti dal contesto applicativo e dal livello di trace attivato.
		X	X	X	X	X	Utilizzo di applicazioni client sviluppate da terzi	Da verificare con il fornitore, potrebbe dipendere dal livello di trace attivato.
		X	X	X	X		Accesso a basi di dati esterne (Agenzia Entrate, Inps/Inail, Bandi Concorsi, Progetti di Ricerca, Statistiche)	Da verificare con il fornitore, potrebbe dipendere dal livello di trace attivato.
X	X	X	X	X	X	X	Utilizzo di piattaforme per l'invio e la consultazione di dati in conservazione digitale	Da verificare con il fornitore, potrebbe dipendere dal livello di trace attivato.
X	X	X	X	X	X	X	Navigazione dell'utente nelle applicazioni Web sviluppate da terzi	Da verificare con il fornitore, potrebbe dipendere dal livello di trace attivato.
			X		X	X	Monitoraggio ai fini statistici dell'accesso ai siti web (es tramite Google Analytics)	Cookie anonimi con registrazione di: lingua di visualizzazione; paese e città di provenienza; browser utilizzato; sistema operativo; provider del servizio internet; risoluzione schermo. Non vengono registrati né l'IP né dati sensibili.

6. SISTEMA DI VIDEOSORVEGLIANZA (se presente)

Le telecamere inquadrano l'ingresso principale sia internamente che esternamente, tutta l'area accessibile e il magazzino. Le immagini possono essere visionate attraverso un monitor o con altri strumenti. Il sistema effettua la videoregistrazione delle immagini per un tempo non superiore alla settimana prolungabile nelle festività.

Liceità

Il trattamento dei dati attraverso il sistema di videosorveglianza è fondato su uno dei presupposti di liceità che il codice prevede espressivamente per soggetti privati ed enti pubblici economici.(adempimento ad un obbligo di legge, provvedimento del Garante di c.d. " bilanciamento di interessi" o consenso libero ad espresso: art. 23-27). La videosorveglianza avviene nel rispetto , oltre che nella disciplina in materia dei protezione dati , di quanto prescritto da altre disposizioni di legge da osservare in caso di installazione di apparecchi audiovisivi (norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata , di tutela della dignità , dell'immagine del domicilio e degli altri luoghi cui è riconosciuta analoga tutela (toilette, stanze d'albergo, cabine, spogliatoi , ecc..) enorme riguardante la tutela dei lavoratori, con particolare riferimento alla legge 300/1970 (statuto dei lavoratori). Il sistema è stato e autorizzato dall'autorità competente.

Finalità

Gli scopi perseguiti sono determinati, espliciti e legittimi e sono volti a migliorare il controllo della sicurezza degli ambienti ad accesso pubblico ed al controllo degli accessi con l'obiettivo di dissuadere eventuali tentativi di furto nei momenti di apertura e/o chiusura. Le finalità sono determinate e rese trasparenti, e quindi direttamente conoscibili attraverso cartelli di avvertimento al pubblico e riportate nell'informativa.

Criteri e modalità di ripristino dei dati, in seguito a distruzione o danneggiamento

Il responsabile della sicurezza dei dati personali ai fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, stabilisce la periodicità con cui debbono essere effettuate le copie di sicurezza delle banche dati trattati.

I criteri sono definiti in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

Salvataggio:

Banca dati	**Luogo di custodia delle copie**	**Struttura incaricata del salvataggio**
Tutte	Sede Principale	Responsabile
Procedura: Back-up effettuato tramite una procedura automatica integrata la quale viene attivata con frequenza giornaliera.		

Il responsabile della sicurezza dei dati personali deve informare il Titolare del trattamento dati affidati all'esterno alla struttura del titolare, dei compiti che gli sono assegnati in relazione a quanto disposto dalle normative in vigore.

DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA'

Titolare del trattamento

Il titolare del trattamento dei dati personali, ai fini della sicurezza, ha le seguenti responsabilità:

- deve nominare per iscritto gli "incaricati" al trattamento dei dati e gli eventuali "responsabili" fornendo le relative istruzioni volte a rispettare le misure di sicurezza.
- Annualmente verifica l'individuazione dell'ambito del trattamento consentito degli incaricati.
- Ha cura dell'attuazione delle misure di sicurezza che sarà necessario adottare personalmente o attraverso soggetti a ciò delegati. Ogni qualvolta è affidata a soggetti esterni l'applicazione delle misure di sicurezza (ad es. consulenti informatici) esterni, il titolare deve ottenere una descrizione scritta degli interventi effettuati che attesti l'operazione effettuata e la conformità alle disposizioni del presente disciplinare.
- Deve vigilare sul rispetto delle proprie istruzioni da parte degli incaricati e degli eventuali responsabili, nonché sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
- Promuove lo sviluppo, la realizzazione ed il mantenimento dei programmi di sicurezza contenuti nel presente Documento dei dati personali;
- Promuove lo svolgimento di un programma di interventi formativi degli incaricati concernenti la sicurezza dei dati mediante l'illustrazione del DPS e delle sue regole di sicurezza. In particolare la previsione di interventi formativi è volta a rendere edotti gli incaricati 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 minime adottate dal titolare. La formazione è programmata già al momento

dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

- Informare gli incaricati sul contenuto del presente documento.

Incaricati del trattamento

Gli incaricati del trattamento dei dati personali, con specifico riferimento alla sicurezza, hanno le seguenti responsabilità:

- svolgere le attività previste dai trattamenti secondo le direttive scritte dal titolare;
- non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del titolare del trattamento;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il titolare in caso di incidenti che dovessero coinvolgere i dati personali.

Tutti gli incaricati devono rispettare le soluzioni previste dal titolare volte a tutelare nel miglior modo possibile la riservatezza dei dati personali dei clienti.

Devono cioè:

- contribuire a far rispettare ai clienti le distanze di cortesia;
- usare ogni cautela che ritengano necessaria volta ad evitare che le prestazioni sanitarie, ivi compresa l'eventuale documentazione di anamnesi, avvenga in situazioni di promiscuità;
- rispettare la dignità dell'interessato in ogni operazione del trattamento;
- fornire informazioni solo ai diretti interessati;
- assumere regole di condotta analoghe al segreto professionale.

Custode delle credenziali di autenticazione informatica

Il custode delle copie delle credenziali di autenticazione informatica è il

Responsabile Trattamento Dati. Il custode ha l'incarico di conservare con segretezza e sotto la propria diretta responsabilità le buste contenti l'indicazione della parola chiave scelta dai singoli incaricati. Il custode deve garantirne la relativa segretezza e informare l'incaricato in caso di necessità. In questo caso l'incaricato dovrà scegliere una nuova credenziale e procedere ad una nuova consegna in busta chiusa al custode.

Responsabili del trattamento esterni

L'organizzazione effettua i trattamenti di dati sensibili mediante strumenti elettronici di seguito elencati, avvalendosi di soggetti esterni nominati responsabili del trattamento:

Trattamento
Gestione dipendenti (elaborazione busta paga contenente informazioni idonee a rivelare l'adesione ad un sindacato, ecc).
Medicina del Lavoro
Studio Commercialista

I compiti affidati al responsabile del trattamento sono analiticamente descritti nella lettera di designazione. Il responsabile del trattamento all'atto dell'affidamento dell'incarico, dichiara per iscritto:

- di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali;
- di ottemperare agli obblighi previsti dal Codice per la protezione dei dati

personali;

- di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere;
- di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze;
- di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

7. DPIA – DATA PROTECTION IMPACT ASSESSMENT

L'analisi dei rischi è stata sviluppata nell'allegato documento dal Responsabile Trattamento Dati ed ha gestito le seguenti situazioni:

- incendio;
- allagamento;
- uragani;
- terremoti;
- fulmini;
- polvere, corrosione, congelamento;
- disturbi elettromagnetici;
- indisponibilità del personale;
- errori di manutenzione hardware e software;
- errori di manutenzione hardware e software;
- errori degli utenti business;
- rilevazione di informazioni (da parte del personale);
- rottura sistema di condizionamento;
- perdita di energia / sbalzi di tensione;
- problemi/sovraccarichi/danni alle apparecchiature e alle linee di TLC;
- malfunzionamenti hardware/software;
- distruzione volontaria di attrezzature;
- furto/intercettazione di informazioni cartacee;
- furto/intercettazione di informazioni digitali;

- furto di apparati e componenti;
- virus;
- hacker;
- uso non autorizzato della strumentazione e dei servizi;
- importazione o esportazione illegale di software (copia illegale di software);
- alterazione volontaria e non autorizzata di dati di business;
- ricezione dati da origine non affidabili;
- ripudio dei messaggi.

Le contromisure messe in atto riguardano:

- classificazione delle informazioni;
- vincoli organizzativi e contrattuali;
- regolamenti e procedure;
- corsi di formazione;
- accesso fisico agli uffici;
- accesso fisico agli archivi cartacei;
- accesso fisico alle sale macchine;
- gestione hardware;
- linee di telecomunicazione;
- protezione della navigazione web;
- protezione dei servizi mail;
- gestione dei gruppi di continuità;
- gestione dei condizionatori;
- gestione dei supporti rimovibili;
- gestione dei dispositivi mobili;
- controllo degli accessi ai servizi informativi alla rete locale;
- accesso remoto;
- protezione degli endpoint;
- log;
- ambienti di sviluppo, test e produzione;
- trasferimento ed invio delle informazioni digitali;
- backup.

Si possono inoltre apprezzare gli accorgimenti adottati per ridurre i rischi:

- software con password e accessi autorizzati;
- backup e backup in remoto;
- antivirus aggiornati;
- firewall gestito;
- password di collegamento al personal computer (Windows) gestite dal Custode delle Password
- password di accesso alla Posta elettronica gestite dal Custode delle Password
- locali ad accesso limitato con sistemi di allarme.

La valutazione dei rischi, oltre che analiticamente, è stata effettuata definendo numericamente un valore dei rischio **(R)**, dato dal prodotto dei due fattori **(P)** e **(D)**, ossia rispettivamente la probabilità che si verifichi un dato evento ed il danno potenziale derivabile dall'evento considerato, secondo i valori di seguito indicati:

DANNO

Gravità	Valore	Definizione
Lieve	**1**	Infortunio o inabilità temporanea con effetti rapidamente reversibili. Esposizione cronica con effetti rapidamente reversibili.
Significativo	**2**	Infortunio o inabilità temporanea con disturbi o lesioni significative reversibili a medio termine. Esposizione cronica con effetti reversibili.
Grave	**3**	Infortunio o inabilità temporanea con lesioni significative irreversibili o invalidità parziale. Esposizione cronica con effetti irreversibili o parzialmente invalidanti.
Gravissimo	**4**	Infortunio con lesioni molto gravi irreversibili e invalidità totale o conseguenze letali Esposizione cronica con effetti letali o totalmente invalidanti.

PROBABILITA'

Probabilità	Valore	Definizione
Improbabile	**1**	Non sono noti episodi già verificati, e/o Il danno si può verificare solo per una concatenazione di eventi improbabili e tra loro indipendenti, e/o Il verificarsi del danno susciterebbe incredulità in azienda
Poco probabile	**2**	Sono noti rari episodi già verificati, e/o Il danno può verificarsi solo in circostanze particolari Il verificarsi del danno susciterebbe sorpresa in azienda
Probabile	**3**	E' noto qualche episodio in cui il pericolo ha causato danno, e/o Il pericolo può trasformarsi in danno anche se non in modo automatico, e/o Il verificarsi del danno susciterebbe scarsa sorpresa in azienda
Molto probabile	**4**	Sono noti episodi in cui il pericolo ha causato danno, e/o Il pericolo può trasformarsi in danno con una correlazione, e/o diretta Il verificarsi del danno non susciterebbe sorpresa in azienda

ECA

RISCHIO

	Probabilità				
Danno		1	2	3	4
	1	**1**	**2**	**3**	**4**
	2	**2**	**4**	**6**	**8**
	3	**3**	**6**	**9**	**12**
	4	**4**	**8**	**12**	**16**

Livello di rischio		**Misure**
11-16	**Rischio altissimo**	- Attuare misure immediate di prevenzione e protezione dai rischi (nell'impossibilità: bloccare temporaneamente il processo produttivo). - Identificare misure di miglioramento nel breve periodo ai fini della riduzione del livello di rischio
5-10	**Rischio alto**	- Attuare misure immediate di prevenzione e protezione dai rischi. - Identificare misure di miglioramento ai fini della riduzione del livello di rischio.
3-4	**Rischio medio**	*Nel caso di rischio con D (pari a 1 o 2) basso:* - Prendere in considerazione misure di miglioramento ai fini della riduzione del livello di rischio. *Nel caso di rischio che presenti D elevato (pari a 3 o 4):* - Attuare misure immediate di protezione dai rischi. - Prendere in considerazione misure di miglioramento ai fini della riduzione del livello di rischio.
1-2	**Rischio basso**	Non sono strettamente necessarie misure di prevenzione e protezione (quelle in atto si possono ritenere sufficienti)

IMPORTANTE: i valori ottenuti **(R)** sono relativi a valutazioni tecniche dei singoli rischi in esame, per cui un basso valore numerico del rischio, considerando costante la probabilità che accada l'evento, non necessariamente può riscontrarsi nella reale entità del danno, poiché stimata probabilisticamente; tale precisazione impone che vengano utilizzati i dati forniti, **per identificare una scala di priorità degli interventi preventivi o protettivi da attuare nel tempo.**

Oltre alla considerazione relativa ai "valori di rischio", per il piano di programmazione degli interventi, si dovrà fare attenzione alla terminologia utilizzata nel documento per indicare gli stessi.

Per quanto concerne gli **strumenti impiegati per il trattamento**, le componenti di rischio possono essere idealmente suddivise come descritto nel documento esterno "ANALISI DEI RISCHI".

Nell'elaborare il modulo si è tenuto conto anche dei seguenti fattori legati alla struttura:

il rischio d'area, legato alla eventualità che persone non autorizzate possano accedere nei locali in cui si svolge il trattamento, è giudicato inferiore per l'area ad accesso controllato, all'interno della palazzina, rispetto a quanto accade per gli altri luoghi in cui si svolge l'attività, con conseguente diminuzione del rischio:

- per gli archivi esistenti in tale area;
- per gli elaboratori in rete privata, in relazione al fatto che i server sono ubicati in tale area;
- per i personal computer non in rete, localizzati in tale area.

Aggiornamento dei programmi

Almeno semestralmente devono essere effettuati gli aggiornamenti dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti. Il Resp. è incaricata di seguire il corretto aggiornamento del software antivirus, del sistema operativo e di altri eventuali software utilizzati correntemente.

Ripristino della disponibilità dei dati sensibili in seguito a distruzione o danneggiamento (disaster recovery)

Il tempo necessario per recuperare i dati delle copie di sicurezza, a fronte di una generica emergenza, è di 3 giorni max. dal verificarsi del possibile accadimento negativo.

Supporti rimovibili contenenti dati sensibili

Tutti i supporti magnetici riutilizzabili (dischetti, cd rom, dvd, cassette, cartucce) contenenti dati sensibili vengono trattati con particolare cautela. Il supporto,

deve essere conservato in armadio chiuso a chiave. Le chiavi sono consegnate per effettuare i trattamenti ivi elencati. Non sono consentiti trattamenti ulteriori. I supporti rimovibili se non utilizzati, devono essere distrutti fisicamente a meno che le informazioni contenute siano rese intelleggibili e sia tecnicamente impossibile ricostruire i dati contenuti.

Protezione delle aree e dei locali

E' garantita la protezione dei locali nei quali è ubicata l'azienda e i dispositivi utilizzati contro i rischi che possono portare alla perdita o alla distruzione dei dati come ad esempio i rischi che si corrono in caso di furto incendio, ecc. (Es. adozione di sistemi di antifurto, serrature particolari ecc., istallazione di estintori ecc..)

7. REVISIONE DEL DOCUMENTO

Il presente documento **deve essere aggiornato se** esigenze operative rendessero necessari aggiornamenti più frequenti, il Titolare si riserva la possibilità di allegare documenti aggiuntivi ad integrazione dello stesso e che ne diventano pertanto parte integrante.

Riepilogo degli adempimenti e delle priorità di intervento

La principale novità introdotta dal regolamento è il principio di "responsabilizzazione" (cd. accountability), che attribuisce direttamente ai titolari del trattamento il compito di assicurare, ed essere in grado di dimostrare, il rispetto dei principi applicabili al trattamento dei dati personali (art. 5). In quest'ottica, la nuova disciplina impone alle amministrazioni un diverso approccio nel trattamento dei dati personali, prevede nuovi adempimenti e richiede un'intensa attività di adeguamento, preliminare alla sua definitiva applicazione a partire dal 25 maggio 2018. Al fine di fornire un primo orientamento, il Garante per la protezione dei dati personali ha suggerito di avviare con assoluta priorità:

⇒ la designazione del Responsabile della protezione dei dati – RPD (artt. 37-39)

⇒ l'istituzione del Registro delle attività di trattamento (art. 30 e cons. 171)

⇒ la notifica delle violazioni dei dati personali (cd. data breach, art. 33 e 34)

ISTITUZIONE DEL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

È essenziale avviare quanto prima le attività idonee ad adottare un registro delle attività di trattamento. In particolare, queste potrebbero consistere nelle attività di seguito descritte:

Attività previste entro il 25 maggio 2018	Descrizione delle attività
Selezione del software usato per il Registro	Sarà necessario individuare una soluzione informatizzata per la gestione del registro delle attività di trattamento. Il registro, infatti, non può essere cartaceo.
Individuazione di eventuali "referenti privacy" per ciascuna struttura d'Azienda	Per favorire la ricognizione dei trattamenti svolti dalle diverse strutture e delle principali caratteristiche di tali trattamenti, è consigliabile chiedere l'individuazione di almeno un "referente privacy" per ciascuna struttura (cioè un dipendente che possa interfacciarsi con il Responsabile della protezione dei dati per tutti gli aspetti concernenti la protezione dei dati trattati dalla struttura di appartenenza).
Ricognizione dei trattamenti svolti e delle loro principali caratteristiche	Per ciascun trattamento dovranno essere individuati seguenti elementi: finalità del trattamento, descrizione delle categorie di dati e interessati, categorie di destinatari cui è prevista la comunicazione, misure di sicurezza, tempi di conservazione, e ogni altra informazione che il titolare ritenga opportuna al fine di documentare le attività di trattamento svolte
Redazione piano di conformità al GDPR	La ricognizione dei trattamenti dovrebbe essere l'occasione per verificare anche il rispetto dei principi fondamentali del GDPR (art. 5), la liceità del trattamento (verifica dell'idoneità della base giuridica, artt. 6, 9 e 10) nonché l'opportunità dell'introduzione di misure a protezione dei dati fin dalla progettazione e per impostazione (privacy by design e by default, art. 25), in modo da assicurare, entro il 25 maggio 2018, la piena conformità dei trattamenti in corso (cons. 171).

NOTIFICA DELLE VIOLAZIONI DEI DATI PERSONALI

Attività previste entro il 25 maggio 2018 in merito alla notifica	Descrizione delle attività
Redazione procedure per la notifica delle violazioni	È necessario individuare idonee procedure organizzative per dare attuazione alle nuove disposizioni sulla notifica delle violazioni dei dati personali (cd. data breach, art. 33 e 34) in cui siano chiariti i seguenti elementi: - Modalità per contattare il Responsabile della Protezione dei dati nel caso di violazioni e tempi di intervento - Casi esemplificativi in cui si rende necessaria la violazione - Casi in cui risulti improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà dell'interessato - Casi e elementi utili a valutare se esiste un "rischio elevato" per i diritti e le libertà dell'interessato - Misure considerate sufficienti per - Individuazione di modalità per effettuare una comunicazione pubblica nell'eventualità indicati all'art. 34 comma 3 lettera c) del GDPR.
Diffusione istruzioni	Data la complessità della nostra azienda è di fondamentale importanza individuare gli strumenti più idonei a favorire la conoscenza delle procedure per la notifica delle violazioni da parte di tutte le persone che trattano dati di titolarità.

Data:

Firma Resp. Trattamenti Dati

Firma Titolare Trattamenti Dati

ECA