ENERGIE PER LA CITTA' SPA

REGOLAMENTO

IMPLEMENTAZIONE, NEL SISTEMA ORGANIZZATIVO AZIENDALE, DI UN SISTEMA DI GESTIONE DELLA PRIVACY IN ADEGUAMENTO AL REGOLAMENTO UE N. 679/2016 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI, NONCHE' ALLA LIBERA CIRCOLAZIONE DI TALI DATI E CHE ABROGA LA DIRETTIVA 95/46/CE

INTRODUZIONE

***

Il presente regolamento (d'ora innanzi per brevità il "**Regolamento**"), recepisce le disposizioni del Regolamento UE 679/2016 (d'ora innanzi per brevità "**GDPR**"), nell'intento di semplificare la loro adozione interna, al fine di garantire il rispetto delle norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Per quanto riguarda le nomine e le figure preposte a tutela e garanzia del rispetto delle disposizioni, sinteticamente, si riportando nel seguito le principali definizioni del nuovo Regolamento con la precisazione che le nomine dei responsabili ed incaricati dei trattamenti, verranno rilasciate da Energie per la Città S.p.A., e per essa dal suo legale rappresentante pro tempre, quale *Titolare del trattamento*.

L'adozione di ulteriori attività di adeguamento, verranno valutate ed eventualmente adottate successivamente all'emanazione, da parte del Garante per la protezione dei dati personali, dopo l'entrata in vigore del D.lgs. n. 101/2018 che coordina la normativa nazionale previgente con GDPR, di nuove linee guida o chiarimenti in ordine al recepimento della normativa europea.

Ambito soggettivo di applicazione: il presente Regolamento si applica a tutti i dipendenti, incaricati, collaboratori, componenti degli organi amministrativi e di controllo della società e a tutti coloro che, nell'esercizio delle proprie mansioni, attività ed a qualsiasi titolo, svolgono attività in qualità di soggetto autorizzato al trattamento dei dati personali comuni e categorie particolari di dati personali ai sensi dell'art. 4 e dell'art. 9 del GDPR; a coloro che sono comunque, addetti alla gestione e/o alla manutenzione degli strumenti elettronici e/o siano stati specificatamente nominati *Amministratore di sistema* e comunque, a tutti coloro, incluse le persone giuridiche, che trattano, in qualsiasi ruolo, dati personali e sensibili di titolarità di

Energie per la Città S.p.A., anche in qualità di *Responsabile esterno del trattamento* ai sensi dell'art. 28 del GDPR.

Ambito oggettivo di applicazione: il Regolamento si applica alle attività che comportano il trattamento dei dati personali quali, ad es. nell'ambito di attività connesse alla gestione del personale, agli organi societari ed agli adempimenti relativi ai fornitori ed eventuali consulenti, per cui Energie per la Città S.p.A. assume la qualifica di *Titolare del trattamento* dei dati.

Titolare del trattamento: è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità ed i mezzi del trattamento di dati personali, quando le finalità ed i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri. Nel caso di Energie per la Città S.p.A., il *Titolare del trattamento*, stante il principio *tempus regit actum*, è individuato nella figura del legale rappresentante *pro tempore*.

Responsabile del trattamento: è la persona fisica che tratta dati personali per conto del *Titolare del trattamento* ai fini organizzativi e aziendali. Nominato come da fac-simile in "Allegato A".

Responsabile esterno del trattamento: è la persona fisica o giuridica che tratta dati personali per conto del *Titolare del trattamento*, in particolare, nel caso di affidamento di appalti di servizi, di forniture, di lavori. La nomina è generalmente effettuata dal *Titolare del trattamento*; ovvero, per conto del .*Titolare del trattamento*, in caso di affidamento, può essere effettuata anche dal *Responsabile del trattamento* quale RUP dell'incarico. Nominato come da fac-simile in "Allegato B".

Soggetto autorizzato al trattamento: persone fisiche, individuabili nei dipendenti che non sono figure apicali, autorizzate al trattamento dei dati personali sotto l'autorità diretta del *Titolare del trattamento* o del *Responsabile del trattamento*. La nomina è effettuata da parte del *Titolare del trattamento* come da fac-simile in "Allegato C".

Amministratore di sistema: è la persona fisica o giuridica nominata ai sensi del provvedimento dell'Autorità Garante del 27 novembre 2008, recante le "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema e s.m.i.". Nonostante l'entrata in vigore del GDPR, permane l'efficacia dei provvedimenti dell'Autorità Garante del 27 novembre 2008 per da nomina dell'Amministratore di Sistema ed il provvedimento della medesima Autorità del 8 aprile 2010 in materia di videosorveglianza. La nomina è effettuata da parte del *Titolare del trattamento* come da fac-simile in "Allegato D".

L'introduzione del presente Regolamento sarà inoltre supportata da un intervento formativo, in modo da renderne edotta l'intera struttura aziendale.

-ARTICOLO 1-

OGGETTO DEL REGOLAMENTO

Il presente Regolamento definisce la disciplina interna atta garantire che il trattamento dei dati personali, svolto nell'ambito delle mansioni lavorative, avvenga nel rispetto dei principi del GDPR che, con decorrenza 25 maggio 2018, integra, a tutti gli effetti, il D.lgs. 196/2003. Il Regolamento si applica secondo i richiamati ambiti soggettivo e oggettivo e, comunque, a tutti coloro, incluse le persone giuridiche, che trattano, in qualsiasi ruolo, dati personali e sensibili di titolarità di Energie per la Città S.p.A., anche in qualità di *Responsabile esterno del trattamento* ai sensi dell'art. 28 del GDPR. Il presente Regolamento si applica inoltre, a tutti coloro che, anche mediante accesso alla rete informatica, utilizzano strumenti elettronici e soluzioni tecnologiche o usufruiscono di servizi la cui sicurezza è gestita da Energie per la Città S.p.A.

-ARTICOLO 2-

ULTERIORI DEFINIZIONI DEL REGOLAMENTO

"**Archivio**": qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

"**Autorità di controllo**": l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 GDPR. In Italia è identificato con il Garante per la protezione dei dati personali.

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

"**Dati genetici**": i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

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

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

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

dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

"**Gruppo imprenditoriale**": un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate.

"**Impresa**": la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica.

"**Limitazione di trattamento**": il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.

"**Norme vincolanti d'impresa**": le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune.

"**Profilazione**": qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

"**Pseudonimizzazione**": il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

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

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

"**Rappresentante**": la persona fisica o giuridica stabilita nell'Unione Europea che, designata dal Titolare del trattamento o dal Responsabile del trattamento per iscritto ai sensi dell'articolo 27 del GDPR, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente Regolamento.

"**Stabilimento principale**": per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione Europea, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione Europea e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale.

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

-ARTICOLO 3-

PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI

Ai sensi del GDPR, articoli 5 e seguenti, i dati personali devono essere:

- ✓ trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
- ✓ raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- ✓ adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
- ✓ esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
- ✓ conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal GDPR a tutela dei diritti e delle libertà dell'interessato;
- ✓ trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Il *Titolare del trattamento* è competente per il rispetto dei suddetti principi e in grado di comprovarlo («responsabilizzazione»).

L'art. 6 del GDPR, precisa i principi che assicurano la liceità del trattamento. Un trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

1) l’interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
2) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
3) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
4) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
5) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
6) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

-ARTICOLO 4-

CONSENSO DELL'INTERESSATO

II consenso dell'interessato costituisce, ai sensi dell'art. 7 del GDPR, qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

In particolare, “Allegato E” e “Allegato F” costituiscono il fac-simile che il *Titolare del trattamento*, e per esso un responsabile o incaricato, deve rilasciare (A) ai dipendenti in caso di assunzione e (B) ai fornitori in caso di procedura di affidamento ai sensi del D.lgs. n. 50/2016 (“**Codice dei Contratti**”), trattandosi dei casi in cui maggiormente la società tratta dati personali. Stessa informativa, di cui all’”Allegato G”, dovrà essere rilasciata ai soggetti cui la società presta od esegue i propri servizi

ed ai componenti nominati degli organi societari e di controllo. La stessa dovrà inoltre essere affissa presso i locali aziendali e le zone aperte al pubblico in modo da essere sempre consultabile.

Informative sulla modalità di trattamento dei dati personali e sull'utilizzo dei cd. "cookie", sono pubblicate sui siti internet della società: www.energieperlacitta.com e www.losportelloexc.it.

-ARTICOLO 5-

DIRITTI DELL'INTERESSATO

I diritti dell'interessato sono trattati agli articoli 12 e seguenti del GDPR. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

L'interessato ha diritto di ottenere l'indicazione:

1) dell'origine dei dati personali;
2) delle finalità, la base giuridica e le modalità del trattamento ed il termine di conservazione dei dati;
3) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
4) degli estremi identificativi del titolare, dei responsabili e del DPO (ove nominato);
5) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato.

L'interessato ha diritto di ottenere:

a) l'accesso, l'aggiornamento, la rettificazione, ovvero, quando vi ha interesse, l'integrazione dei dati;

b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
c) il diritto all'oblio e la profilazione dei dati nel caso di trattamento automatizzato;
d) il diritto di revocare il consenso espresso.

L'interessato ha diritto di opporsi, in tutto o in parte:

- ✓ per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
- ✓ al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Tali diritti sono esercitati con richiesta rivolta senza formalità al *Titolare del trattamento*, tenuto a fornire idoneo riscontro senza ritardo.

La richiesta può essere trasmessa senza formalità e, quindi, anche mediante lettera raccomandata, telefax o posta elettronica. Il Garante può individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche; la richiesta può essere formulata anche oralmente e in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile.

Nell'esercizio dei diritti di accesso l'interessato può conferire, per iscritto, delega e altresì, farsi assistere da una persona di fiducia.

I diritti di accesso riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

L'identità dell'interessato è verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento.

La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato.

I dati sono estratti a cura del responsabile o degli incaricati e comunicati agli interessati; possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni.

Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica.

Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare.

Il riscontro alla richiesta dell'interessato può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti.

Il diritto di ottenere la comunicazione in forma intelligibile dei dati non riguarda dati personali relativi a terzi, salvo che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.

La comunicazione dei dati è effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile. In caso di comunicazione di codici o sigle sono forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato.

-ARTICOLO 6-

L'AMMINISTRATORE DI SISTEMA

In data 27.11.2008 il Garante ha emanato uno specifico provvedimento denominato "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti

elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".

Tale provvedimento, come modificato dal successivo provvedimento del 25.06.2009, è ancora vigente nonostante il nuovo GDPR.

E', quindi, il Garante che in detto provvedimento prevede che con la definizione di *Amministratore di Sistema* si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti.

Ai fini del provvedimento del Garante vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Viene nominato dal *Titolare del trattamento* secondo l'"Allegato D".

-ARTICOLO 7-

VIDEOSORVEGLIANZA

Il provvedimento del Garante del 8.04.2010 e le successive linee guida, al momento, disciplinano ancora l'utilizzo dei sistemi di videosorveglianza.

Il Garante ha emanato, infatti, anche delle linee guida contenenti gli indirizzi per garantire che l'installazione di dispositivi per la videosorveglianza rispetti le norme sulla privacy e sulla tutela della libertà delle persone, in particolare assicurando la proporzionalità tra mezzi impiegati e fini perseguiti.

La materia è stata poi ulteriormente regolata da due provvedimenti generali del Garante, che contengono prescrizioni vincolanti per tutti i soggetti che intendono avvalersi di sistemi di videosorveglianza e precise garanzie per la privacy dei soggetti i cui dati vengano eventualmente raccolti e trattati tramite tali sistemi.

Secondo tutti i citati provvedimenti, i soggetti che transitano nelle aree sorvegliate devono essere informati con cartelli della presenza delle telecamere, i cartelli devono

essere resi visibili anche quando il sistema di videosorveglianza è attivo in orario notturno.

Nel caso in cui i sistemi di videosorveglianza installati siano collegati alle forze di polizia è necessario apporre uno specifico cartello sulla base del modello elaborato dal Garante.

Si segnala che l'informativa ai dipendenti non esime dall'attivazione prevista dall'art. 4 dello Statuto dei Lavoratori.

Con la Pubblicazione nella Gazzetta Ufficiale del 23.09.2015 (Suppl. Ordinario n. 53), è entrato in vigore il Decreto Legislativo n. 151 del 14 settembre 2015, recante «Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità, in attuazione della legge 10 dicembre 2014 n. 183».

L'articolo 23 del D.Lgs. n. 151/2015 ha modificato l'articolo 4 della Legge n. 300 del 1970 - anche nota come Statuto dei Lavoratori - per rimodulare la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener

conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti «dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori» e di quelli «utilizzati dal lavoratore per rendere la prestazione lavorativa».

Per quanto riguarda l'installazione e l'utilizzo degli strumenti di cui al primo comma, è stata confermata una procedura di codeterminazione fra datore di lavoro e Rappresentanze Sindacali (RSU o RSA) - che trova luogo tramite un Accordo con le rappresentanze sindacali presenti nelle diverse unità produttive dell'azienda ai fini dell'installazione e dell'utilizzo dell'impianto di controllo preliminare rispetto all'installazione degli strumenti, il cui esito negativo porta il datore a richiedere l'autorizzazione amministrativa della DTL competente.

Inoltre, tutte le informazioni raccolte con i mezzi di controllo devono essere utilizzate nel rispetto della disciplina sulla privacy. Infatti il comma 3 del novellato articolo 4 dello Statuto dei Lavoratori, a chiusura della disciplina sui controlli a distanza, prescrive che tali informazioni «sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003/ n. 196» sul trattamento dei dati sensibili.

Per Energie per la Città S.p.A., attualmente, non è installato alcun dispositivo di video sorveglianza.

-ARTICOLO 8-

UTILIZZO DEGLI STRUMENTI INFORMATICI AZIENDALI

L'utilizzo delle risorse informatiche e telematiche aziendali deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro. Energie per la Città S.p.A. ha adottato una procedura interna diretta ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Utilizzo del personal computer.

Il personal computer ("**PC**") affidato al dipendente o al collaboratore è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso al PC è protetto da password che deve essere custodita dall'incaricato con la massima diligenza, non divulgata e cambiata con cadenza semestrale. Ciascun incaricato provvederà, di volta in volta, a consegnare al responsabile incaricato la propria password.

L'*Amministratore di sistema*, per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna.

L'*Amministratore di sistema* potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa azienda, *Titolare del trattamento*, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio, in caso di prolungata assenza o impedimento dell'incaricato.

Non è consentito installare autonomamente programmi provenienti dall'esterno se non previa autorizzazione esplicita dell'*Amministratore di sistema*, in quanto sussiste il grave pericolo di portare virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dall'*Amministratore di sistema* di Energie per la Città S.p.A. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei

diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio personal computer, salvo autorizzazione esplicita dell'*Amministratore di sistema*.

Il PC deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Deve essere attivato lo screen saver (per periodi di inutilizzo >10 minuti), con richiesta di password alla ripresa dell'attività sulla postazione.

Non è consentita l'installazione sul proprio PC di alcun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.), se non con l'autorizzazione espressa dell'*Amministratore di sistema.*

Ogni operatore deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'*Amministratore di sistema* nel caso in cui vengano rilevati virus.

Utilizzo della rete.

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.

Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.

L'*Amministratore di sistema* potrà in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui PC degli incaricati sia sulle unità di rete.

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

È cura dell'operatore effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata. Allo stesso modo è buona regola utilizzare una trita-carta prima di disfarsi di stampe e/o documenti che possano contenere dati personali.

Gestione delle password.

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dall'Amministratore di sistema.

È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi. Ciascun incaricato provvederà, di volta in volta, a consegnare all'Amministratore di sistema le nuove password.

Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

La password deve essere immediatamente sostituita, dandone comunicazione all'*Amministratore di sistema*, nel caso si sospetti che la stessa abbia perso la segretezza.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione o all'*Amministratore di sistema*.

Utilizzo dei supporti magnetici.

Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce) contenenti dati particolari e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

I supporti magnetici contenenti dati particolari e giudiziari devono essere custoditi in archivi chiusi a chiave.

Utilizzo di personal computer portatili.

L'utente è responsabile del PC portatile assegnatogli dalla Direzione e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili utilizzati all'esterno (convegni, visite in azienda, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto.

Uso della posta elettronica.

La casella di posta, assegnata dall'Azienda all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.

È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per Energie per la Città S.p.A. deve essere visionata od autorizzata dalla Direzione, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

La documentazione elettronica che costituisce per l'azienda "knowhow" aziendale tecnico o commerciale protetto, e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (posta elettronica certificata, fax, posta raccomandata).

Per la trasmissione di file all'interno di Energie per la Città S.p.A. è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.

È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente all'*Amministratore di sistema*. Non si devono in alcun caso attivare gli allegati di tali messaggi.

Uso della rete internet e dei relativi servizi.

Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita

la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dall'*Amministratore di sistema*.

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.

È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

-ARTICOLO 9-

REGISTRO DEI TRATTAMENTI

La tenuta del registro dei trattamenti è prevista dall'articolo 30 del GDPR, ed è considerata indice di una corretta gestione dei trattamenti.

L'onere della tenuta del registro è a carico del *Titolare del trattamento* e, se nominato, del *Responsabile del trattamento*. La tenuta del registro è utile per una completa ricognizione e valutazione dei trattamenti svolti e quindi finalizzata anche all'analisi del rischio di tali trattamenti e ad una corretta pianificazione dei trattamenti. .

Il registro deve essere tenuto in forma scritta, anche in formato elettronico, e va esibito all'autorità di controllo (Garante) in caso di verifiche. Sono esentate dall'obbligo di tenuta del registro le imprese o le organizzazioni con meno di 250 dipendenti, a meno che il trattamento effettuato:

~ possa presentare un rischio per i diritti e le libertà degli interessati;

~ non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10 (cioè dati sensibili o giudiziari), del Regolamento UE.

Per ragioni di maggior cautela, Energie per la Città S.p.A. si è dotata di un registro dei trattamenti conservato, in formato elettronico, da aggiornarsi periodicamente in caso di nuovi trattamenti e/o di nuove nomine e disponibile per essere stampato ed esibito.

Contenuto minimo

Il registro deve elencare una serie di informazioni:

1) nome e i dati di contatto del *Titolare del trattamento* e, se nominati, del contitolare del trattamento e del responsabile della protezione dei dati;
2) le finalità del trattamento;
3) una descrizione delle categorie di interessati e categorie di dati personali;
4) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi destinatari di paesi od organizzazioni internazionali;
5) ove applicabile, l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49 del Regolamento UE, la documentazione delle garanzie adeguate;
6) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
7) ove possibile, una descrizione generale delle misure di sicurezza tecniche eorganizzative di cui all'articolo 32, paragrafo 1 del Regolamento.

-ARTICOLO 10-

ISTRUZIONI OPERATIVE DATA BREACH

L'art. 33 del GDPR impone al *Titolare del trattamento* di notificare all'autorità di controllo la violazione di dati personali (cd. "Data Breach"), entro 72 ore dal momento in cui ne viene a conoscenza.

L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il *Titolare del trattamento* è tenuto a darne comunicazione all'interessato.

Il termine per adempiere alla notifica è brevissimo, 72 ore dal momento in cui il *Titolare del trattamento* ne viene a conoscenza, mentre, l'eventuale comunicazione agli interessati, deve essere fatta senza indugio.

L'eventuale ritardo nella notificazione deve essere giustificato, il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti dall'art.58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi di dati), la imposizione di sanzioni amministrative secondo l'art. 83 GDPR.

Per violazione di dati si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (Art. 4 p.12 del GDPR).

La violazione di dati è un particolare tipo di incidente di sicurezza, per effetto del quale, il *Titolare del trattamento* non è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del GDPR per il trattamento dei dati personali.

Preliminarmente, dunque, il *Titolare del trattamento* deve poter identificare l'incidente di sicurezza in genere, quindi, comprendere che l'incidente ha impatto sulle informazioni e, infine, che tra le informazioni coinvolte dall'incidente vi sono dati personali.

L'art. 33 p.5 del GDPR prescrive al *Titolare del trattamento* di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma.

L'art. 33 p.2 GDPR prevede espressamente il dovere per il responsabile, quando viene a conoscenza di una violazione, di informare, senza ingiustificato ritardo, il *Titolare del trattamento*.

È importante che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notifica.

Si possono distinguere tre tipi di violazioni:

1) violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
2) violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
3) violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

Una violazione potrebbe comprendere una o più tipologie.

Per comprendere quando notificare la violazione è opportuno effettuare una valutazione dell'entità dei rischi:

- **Rischio assente**: la notifica al Garante non è obbligatoria.
- **Rischio presente**: è necessaria la notifica al Garante.
- **Rischio elevato**: in presenza di rischi "elevati", è necessaria la comunicazione agli interessati. Nel momento in cui il *Titolare del trattamento* adotta sistemi di crittografia dei dati, e la violazione non comporta l'acquisizione della chiave di decrittografia, la comunicazione ai soggetti interessati non sarà un obbligo.

I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

a) coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
b) riguardare categorie particolari di dati personali;

c) comprendere dati che possono accrescere ulteriormente i potenziali rischi (es. dati di localizzazione, finanziari, relativi alle abitudini e preferenze);

d) comportare rischi imminenti e con un'elevata probabilità di accadimento (es. rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);

e) impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (es. pazienti, minori, soggetti indagati).

Per la notifica della violazione e la comunicazione al Garante occorre compilare gli appositi moduli messi a disposizione.

-ARTICOLO 11-

PUBBLICITA' PER FINALITA' DI TRASPARENZA

Energie per la Città S.p.A. è soggetta alle procedure di cui al Codice dei Contratti e, per quanto di interesse in materia di trattamento di dati personali, agli obblighi di cui al D.lgs. n. 33/2003, cd. Decreto trasparenza, recante "*Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*".

Gli anzidetti trattamenti, oltre allo specifico dovere di informativa e raccolta del consenso come da modello in Allegato F, dovranno essere svolti da ciascun responsabile o incaricato in conformità ai provvedimenti del Garante Privacy:

- 2.03.2011, recante "*Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web*" (pubblicato in G.U. n. 64 del 19 marzo 2011), di cui in "Allegato H", e
- 15.05.2014, recante "*Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati*" di cui in "Allegato I".

-ARTICOLO 12-

CERTIFICATI MEDICI E GIUDIZI DI IDONEITA' AL LAVORO

Energie per la Città S.p.A. nomina il medico responsabile per i dipendenti soggetti a sorveglianza sanitaria e per le altre finalità di cui al D.lgs. 9 aprile 2008 n. 81 "Testo unico sulla salute e sicurezza sul lavoro".

Il Garante ha fornito alcuni chiarimenti nel caso di attestati rilasciati dalle strutture ospedaliere, indicando i requisiti che questi devono avere, e più in particolare, le informazioni che non possono essere contenute al loro interno, al fine di non incorrere in violazione delle regole sulla privacy.

Sui certificati medici rilasciati da enti pubblici devono essere presenti solo informazioni generiche. Questo significa che non vi devono essere dati di carattere personale circa: lo stato di salute del paziente; la tipologia di esame diagnostico effettuato; la tipologia di visita effettuata ecc.

Parimenti, il medico è obbligato a non divulgare a terzi le condizioni di salute dei propri pazienti e, nei certificati medici legali che attestano l'idoneità al servizio di un lavoratore, deve essere riportato il solo giudizio medico legale, senza diagnosi.

Il certificato deve avere carattere generico, senza alcun riferimento agli aspetti personali riguardanti il paziente.

Sarà cura di ogni lavoratore, in caso di consegna di certificati medici, e del medico nominato, a seguito di visite mediche, trasmettere a Energie per la Città S.p.A. solo certificati e giudizi di idoneità conformi alla vigente normativa in materia di privacy.

La Direzione, e per essa il soggetto incaricato, potranno rifiutare di ricevere e conservare certificati e giudizi di idoneità contenenti informazioni non generiche e comunque volte a rivelare lo stato di salute o aspetti personali riguardanti il paziente, richiedendo espressamente la loro sostituzione con altro documento conforme.

-ARTICOLO 13-

OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DI DATI PERSONALI E DELLA NORMATIVA AZIENDALE

È obbligatorio, per tutti i soggetti cui è applicabile il presente Regolamento, attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR. Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento sono perseguibili con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

-ARTICOLO 14-

AGGIORNAMENTO E REVISIONE

Chiunque può proporre, over ritenuto necessario, integrazioni al presente Regolamento. Ogni proposta verrà esaminata dal *Titolare del trattamento*.

Il presente Regolamento che si compone di n. 14 articoli, oltre all'introduzione ed agli allegati citati, è soggetto a revisione con frequenza annuale.