

	CODICE DELLA PRIVACY DPS documento programmatico sulla sicurezza DLGS 196/2006				
S/DSI/GE/0004	0	10/07/09	G.Lana	G.Lana	Pubblico
<i>Codice documento</i>	<i>Rev.</i>	<i>Data</i>	<i>Estensore</i>	<i>Approvato</i>	<i>Uso</i>

Disposizioni minime sulla sicurezza

E

Documento programmatico sulla sicurezza

Il presente documento si compone di n. 22 pagine (inclusa la presente)

Luogo e data: Sesto San Giovanni, 10/07/09

Il responsabile della sicurezza
Giuseppe Lana



Indice

Premessa	2
Attività di Energie Locali S.r.l.	3
Titolare, responsabili, incaricati	3
IL DPS (documento programmatico sulla sicurezza)	4
Istruzioni relative alle tabelle	6
Allegati	22

Premessa

Scopo di questo documento è stabilire le misure di sicurezza organizzative, fisiche e logiche da adottare affinché siano rispettati gli obblighi, in materia di sicurezza del trattamento dei dati effettuati da parte di Energie Locali S.r.l., previsti dal D. L.vo 30/06/2003 N. 196 “Codice in materia di protezione dei dati personali”.

Nella redazione del proprio Documento Programmatico Sulla Sicurezza (d’ora innanzi DPS), Energie Locali S.r.l. ha confermato la scelta di elaborare un documento il più possibile snello, ma, allo stesso tempo coerente con le indicazioni fornite dall’ Ufficio del Garante per la Protezione dei dati personali.

Tale scelta trova origine in due distinte motivazioni:

- Innanzi tutto con la volontà di confrontarsi con uno schema di riferimento predisposto dal soggetto che istituzionalmente ha il compito di vigilare sul rispetto del D.Lgs. 196/2003, da un lato e che, dunque, dovrebbe presentare un’ adeguato standard di intelligibilità e coerenza alle richieste della citata autorità;
- La volontà di considerare il tema della privacy e, di conseguenza, gli obblighi aziendali che ne derivano, come un tema in divenire, che dovrà essere costantemente monitorato nel tempo.

Eventuali situazioni di deviazione accertate rispetto a quanto precisato nel presente documento dovranno essere rimosse nel più breve tempo possibile.



Attività di Energie Locali S.r.l.

Progettazione, realizzazione, manutenzione di impianti di illuminazione pubblica e semaforica, impianti di calore, fornitura energia elettrica.

Titolare, responsabili, incaricati

La figura del titolare (art. 28) coincide con Energie Locali S.r.l. (entità che nel suo complesso esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo sulla sicurezza).

E' responsabile del trattamento, il Sig. Giuseppe Lana , che si avvale del supporto delle varie funzioni aziendali.

Sono invece da considerarsi incaricati del trattamento (art. 30) le persone fisiche (dipendenti, somministrati, consulenti) che, in funzione della diversa collocazione nella struttura organizzativa, trattano i dati, anche in maniera tra loro differenziata nell'ambito del trattamento consentito in funzione delle specifiche istruzioni ricevute.

Sono stati infine individuati (cfr tabella 7 e relative istruzioni) i Titolari/Responsabili esterni per le attività (o parti di attività) che Energie Locali S.r.l. ha, a sua volta affidato in outsourcing.



IL DPS (documento programmatico sulla sicurezza)

Il presente DPS è redatto , ai sensi delle leggi vigenti, per definire le politiche di sicurezza in materia di trattamento dei dati personali, ed i criteri organizzativi per la loro attuazione. In particolare nel Documento programmatico sulla Sicurezza vengono definiti:

- L'elenco dei trattamenti dei dati personali;
- La distribuzione dei compiti e delle responsabilità;
- L'analisi dei rischi che incombono sui dati;
- Le misure in essere e da adottare tra cui i criteri e le procedure per assicurare l'integrità dei dati, i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai medesimi locali, i criteri e le procedure per la sicurezza della trasmissione dei dati;
- I criteri e le procedure per il ripristino della disponibilità dei dati;
- I criteri e le procedure per il salvataggio dei dati;
- L'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni;
- I trattamenti affidati all'esterno.

Campo di applicazione

Il DPS, definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali.

Riguarda tutti i dati:

1. Sensibili
2. Giudiziari
3. Personali e identificativi

Il DPS si applica al trattamento di tutti i dati personali per mezzo di:

- Strumenti elettronici di elaborazione
- Altri strumenti di elaborazione (es. cartacei, audio, visivi e audiovisivi, ecc.)

Il Documento Programmatico Sulla Sicurezza è conosciuto e applicato da tutti gli Uffici della Azienda.

Riferimenti normativi

La redazione del Dps avviene in conformità al già citato riferimento al D. Lgs. 30 giugno 2003, n. 196 (in particolare all'art. 34, lettera g), ed al relativo Allegato B, punto 19. (documentazione disponibile in Azienda).

Approccio metodologico

La redazione del presente DPS avviene sulla base delle seguenti assunzioni:

- L'informazione rappresenta una risorsa aziendale di indiscusso valore che necessita di una tutela adeguata, la cui messa in sicurezza permette di prevenire diverse tipologie di rischio contribuisce sia a garantire la continuità operativa sia a disporre dei dati per il miglioramento



"CODICE DELLA PRIVACY – DPS DLGS 196/03"

- Ciò vale in particolare per l'informazione relativa a dati personali, il cui corretto e finalizzato utilizzo costituisce regola etica fatta propria da Energie Locali S.r.l.
- Il presente DPS non costituisce un punto di arrivo, ma semmai di partenza e necessita di essere costantemente aggiornato in ragione del modificarsi delle situazioni di fatto.

Come anticipato nell'introduzione, al fine di rendere di più facile lettura il DPS è stato scelto di redigere tabelle coerenti con quelle predisposte dall'Ufficio del Garante in data 11.6.2004, procedendo ad attribuire, ove possibile, a ciascuna colonna presente nelle citate tabelle di riferimento, un titolo almeno simile a quello contenuto in quello predisposte dall'ufficio del Garante.

Al fine di razionalizzare e sistematizzare la redazione del DPS si è quindi proceduto a classificare il contenuto di ciascuna colonna in un numero relativamente limitato di variabili, identificate secondo un codice di riconoscimento delle quali verrà più avanti fornita una legenda (si vedano le istruzioni relative alle varie tabelle).

Tale classificazione, peraltro ampliabile o modificabile a fronte di sviluppi fino ad oggi non previsti, ha consentito di rendere più snello il contenuto delle varie tabelle e consentirà una più semplice classificazione di trattamenti/banca dati di nuova costituzione.

Nelle pagine che seguono vengono riportate le istruzioni necessarie per la corretta comprensione delle tabelle, ove necessario arricchite con alcune ulteriori specificazioni metodologiche, di lettura e coordinamento.



Istruzioni relative alle tabelle

Istruzioni relative alla Tabella 1 – Elenco trattamento dei dati personali (reg. 19.1)

Contenuti

In questa sezione sono individuati i trattamenti effettuati dal titolare, direttamente o attraverso collaborazioni esterne, con l'indicazione della natura dei dati e della struttura (ufficio, funzione, ecc.) interna o esterna operativamente preposta, nonché degli strumenti elettronici impiegati.

Informazioni essenziali

Colonna 1 – Identificativo del Trattamento

Si articola in 3 sottocolonne, e cioè:

Colonna 1.1 – Numero progressivo del trattamento/Banca dati

Attribuisce un numero progressivo a ciascun trattamento/Banca dati, per facilitarne l'identificazione.

Colonna 1.2 – Ruolo di Energie Locali S.r.l.

In questa colonna viene specificato se il ruolo di Energie Locali S.r.l. è quello di Titolare (T) o Responsabile (R) del trattamento.

Ad esplicitazione della qualificazione effettuata occorre ricordare che il D. Lgs 196/2003 definisce come titolare colui cui competono le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza, e quello di responsabile colui che è preposto dal titolare al trattamento di dati personali.

Colonna 1.3 - Nome del trattamento/ Banca Dati

Attribuisce a ciascun trattamento/banca dati un nome/ codice che favorisce l'identificazione della banca dati, a eguale regola ci si attiene per le attività affidate in outsourcing da Energie Locali S.r.l.(che trovano un ulteriore approfondimento nella tabella 7). I trattamenti di cui Energie Locali S.r.l. è titolare vengono espressi con la descrizione dell'attività cui sono finalizzate, secondo quanto specificato nella successiva colonna.

Colonna 2 – Descrizione sintetica della finalità perseguita/attività svolta

Si articola in una colonna 2.1 nella quale viene riportato un codice che corrisponde all'attività svolta, ed in una colonna 2.2 nella quale viene riportato un codice relativo alle categorie di interessati.

Le legende dei codici vengono riportate di seguito.

Colonna 2.1

FSI **Fornitura Servizi assistenza interna**
Fornitura di servizi IT di assistenza interna



"CODICE DELLA PRIVACY – DPS DLGS 196/03"

- AC: Anagrafiche clienti**
Registrazione delle fatture clienti e delle proposte di vendita prodotti
- AF: Anagrafiche fornitori**
Registrazione delle fatture fornitori
- DS: Dipendenti somministrati**
Dipendenti somministrati, gestione anagrafica e orario di lavoro dei dipendenti
- RO: Richieste di offerta**
Monitoraggio di potenziali clienti, e gestione dello storico delle offerte formulate al fine di eventuali successivi confronti con progetti assimilabili (in tutto o in parte)
- CONT: Contratti**
Monitoraggio dei contratti, attivi e scaduti
- AP: Amministrazione del personale**
Dare corso agli adempimenti legali e contrattuali in materia di lavoro
- SP: Selezione del Personale**
Raccogliere ed organizzare curricula di potenziali dipendenti/somministrati al fine di valutarne l'inserimento in azienda
- PACO: Paghe e Contributi**
Procedere all'elaborazione delle buste paga per dipendenti e collaboratori, e dare corso ai conseguenti adempimenti assistenziali, previdenziali e fiscali

Colonna 2.2

- ALL: Tutti coloro che interfacciano il sistema informatico aziendale.**
- C1: Committenti/Clienti**
- CO: Competitors**
- DC: Dipendenti/collaboratori**
- F: Fornitori (inclusi i consulenti)**
- PC: Potenziali clienti**

Colonna 3 - Natura dei dati trattati

La colonna è stata distinta in relazione al trattamento di dati sensibili (3.1) e giudiziari (3.2).

In entrambe le colonne il numero 1 indica la presenza di dati di tale natura, il numero 0 l'assenza degli stessi.

Colonna 4 - Struttura di riferimento

Viene indicata, con un codice la cui legenda viene di seguito riportata, la direzione all'interno della quale viene effettuato il trattamento.

Per quanto attiene ai trattamenti affidati all'esterno, si procede alla semplice indicazione di tale affidamento esterno, identificandolo con il codice OUT (outsourcer), che viene poi successivamente identificato in tabella 7.

Considerato che la presente tabella si riferisce alla struttura aziendale che effettua il trattamento, non viene mai indicato in questa colonna il nominativo del committente titolare del trattamento, che può invece comparire (con codice C1,C2 o F) nella colonna successiva.

- DG: Direzione Generale**
- DC: Direzione Commerciale**
- AT: Assistenza Tecnica**
- OUT: Outsourcer**

Colonna 5 – Altre strutture che concorrono al trattamento



"CODICE DELLA PRIVACY – DPS DLGS 196/03"

Vengono indicate:

con il codice la cui legenda viene utilizzata in colonna 4, le direzioni all'interno della quale viene effettuato il trattamento, in caso di intervento interno;

Con il codice **ALL** viene indicato in caso in cui concorrono tutte le direzioni

Con un codice coerente a quello utilizzato in colonna 3.2, il tipo di soggetto esterno, in caso di trattamento esterno

T: **Titolare del trattamento**

OUT: **Outsourcer per conto di Energie Locali**

F: **Fornitori (inclusi i consulenti)**

Colonna 6 – Descrizione degli strumenti utilizzati

Si articola in tre sottocolonne:

Colonna 6.1

Indica, tramite un codice la cui legenda viene di seguito riportata, gli strumenti utilizzati

PC: **Personal Computer**

Colonna 6.2

Indica il tipo di rete, interna od esterna, che, eventualmente, supporta gli strumenti elettronici impiegati

I: **sistema aziendale**

OUT: **sistema esterno dell' outsourcer, responsabile del trattamento**

La colonna 6.2 costituisce fondamentale premessa per la lettura delle successive tabelle. Infatti, nel caso di indicazione di sistema esterno del cliente (T) tutte le tematiche della sicurezza, analisi dei rischi, salvataggio e ripristino di cui alle successive tabelle 3 (per la parte relativa agli eventi relativi agli strumenti) 4 e 5 non vengono sviluppate, in quanto di diretta competenza del proprietario del sistema.

Colonna 6.3

Viene indicato se i dati vengono raccolti in/su:

F: **File**

D: **Database**

C: **Cartaceo**

M: **Mail**



Istruzioni relative alla tabella 2 – Distribuzione dei compiti e delle responsabilità (reg. 19.2)

Contenuti

Vengono sinteticamente descritte le strutture di riferimento, i compiti e le relative responsabilità, in relazione ai trattamenti effettuati.

Informazioni essenziali

Colonna 1 – Struttura

Viene indicata, con un codice la cui legenda viene di seguito riportata, la direzione all'interno della quale viene effettuato il trattamento.

Coincide con le strutture interne indicate nella colonna 4 della tabella 1.

Per comodità si provvede a riportarne la legenda:

DG: Direzione Generale

DC: Direzione Commerciale

AT: Assistenza Tecnica

OUT: Outsourcer

Colonna 2 – identificativo del trattamento

Al fine di facilitare il coordinamento tra questa tabella e la precedente, è articolata esattamente come la colonna 2 di tabella 1.

Si articola in 3 sottocolonne, e cioè:

Colonna 2.1- Numero progressivo del trattamento/banca dati

Attribuisce a ciascun trattamento/banca dati una numerazione progressiva, al fine di facilitarne l'identificazione

Colonna 2.2 Ruolo di Energie Locali S.r.l.

In questa colonna viene specificato se il ruolo di Energie Locali S.r.l. è quello di titolare (T) o responsabile (R) del trattamento.

Ad esplicitazione della qualificazione effettuata occorre ricordare che il D. Lgs 196/2003 definisce come titolare colui cui competono le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza, e quello di responsabile colui che è preposto dal titolare al trattamento di dati personali.

Colonna 2.3- Nome del trattamento/banca dati (colonna nascosta)



"CODICE DELLA PRIVACY – DPS DLGS 196/03"

Attribuisce a ciascun trattamento/banca dati un nome/ codice che favorisce l'identificazione della banca dati.

Nel caso di banche dati necessarie allo svolgimento di attività in outsourcing per conto di clienti il nome contiene l'indicazione del cliente per conto del quale si opera (o di un suo codice identificativo).

(Le attività affidate in outsourcing da Energie Locali S.r.l. trovano invece collocazione nella tabella 7).

La versione integrale del DSP, contenente la colonna nascosta, è a disposizione delle autorità legittimate al controllo del rispetto della normativa sulla tutela della Privacy.

Colonna 3 Trattamenti effettuati dalla struttura, di cui la stessa è responsabile

Vengono costruite 5 sottocolonne.

Colonna 3.1 - inserimento

Comprende, raggruppata sotto la voce inserimento, lo svolgimento di almeno una delle seguenti operazioni:

- a. raccolta (anche cartacea);**
- b. registrazione.**

Lo svolgimento di almeno una di tali operazioni viene indicato con 1 nella colonna; il mancato svolgimento di tutte queste operazioni viene indicato con 0 nella colonna;

Colonna 3.2 -modifica

Comprende, raggruppata sotto la voce modifica, lo svolgimento di almeno una delle seguenti operazioni:

- a. blocco;**
- b. Modificazione.**

Lo svolgimento di almeno una di tali operazioni viene indicato con 1 nella colonna; il mancato svolgimento di tutte queste operazioni viene indicato con 0 nella colonna;

Colonna 3.3 -consultazione

Comprende, raggruppata sotto la voce consultazione, lo svolgimento delle attività di consultazione

- a. Consultazione;**
- b. raffronto.**

Lo svolgimento di almeno una di tali operazioni viene indicato con 1 nella colonna; il mancato svolgimento di tutte queste operazioni viene indicato con 0 nella colonna;

Colonna 3.4 -elaborazione

Comprende, raggruppata sotto la voce elaborazione, lo svolgimento di almeno una delle seguenti operazioni:

- a. elaborazione**
- b. estrazione**
- c. selezione**
- d. raffronto**
- e. interconnessione**

Lo svolgimento di almeno una di tali operazioni viene indicato con 1 nella colonna; il mancato svolgimento di tutte queste operazioni viene indicato con 0 nella colonna;



"CODICE DELLA PRIVACY – DPS DLGS 196/03"

Colonna 3.5 - distruzione

Comprende, raggruppata sotto la voce distruzione, lo svolgimento di almeno una delle seguenti operazioni:

blocco;
cancellazione;
distruzione.

Lo svolgimento di almeno una di tali operazioni viene indicato con 1 nella colonna; il mancato svolgimento di tutte queste operazioni viene indicato con 0 nella colonna;

L'identificazione in responsabilità in materia di manutenzione tecnica dei programmi e di gestione tecnica operativa della base dati (salvataggi, ripristini, ecc) vengono invece specificate nella successiva colonna 4.

Colonna 4 – ulteriori responsabilità in materia di sicurezza

La presente colonna, compilata esclusivamente nel caso di trattamenti effettuati con strumenti elettronici, individua la competenza e responsabilità circa:

Colonna 4.1 - manutenzione tecnica dei programmi.

Colonna 4.2 - gestione tecnica operativa della base dati (salvataggi, ripristini, ecc.)

In queste colonne viene specificato il soggetto responsabile con riferimento a ciascuno dei due aspetti, indicato con il codice già specificato della direzione già utilizzata in colonna 1 se interno, o con le lettera:

T: Titolare
FP: Fornitore del programma
OUT: Outsourcer

in caso di soggetto esterno (identificabile, ove T, sulla base alla colonna nascosta 2.3).



Istruzioni relative alla tabella 3 – Analisi dei rischi che incombono sui dati (reg. 19.3)

Contenuti

Vengono descritti i principali eventi potenzialmente dannosi per la sicurezza dei dati, le loro possibili conseguenze e la gravità in relazione al contesto fisico-ambientale di riferimento e agli strumenti elettronici utilizzati.

Informazioni essenziali

Colonna 1 - Indicazione della tipologia dei rischi

La colonna è stata ulteriormente divisa in 2 parti:

Colonna 1.1:

raggruppa i rischi per macroaree, sulla base della seguente tripartizione, sulla base delle indicazioni fornite dall'Ufficio del Garante:

- 1.A: comportamenti degli operatori;**
- 1.B: eventi relativi agli strumenti;**
- 1.C: eventi relativi al contesto;**

Colonna 1.2:

dettaglia ulteriormente i possibili rischi:

- R.A.1:** sottrazione di credenziali di autenticazione
- R.A.2:** carenza di consapevolezza, disattenzione, incuria
- R.A.3:** comportamenti sleali o fraudolenti
- R.A.4:** errore materiale
- R.A.5:** altro evento

- R.B.1:** azione di virus informatici o di programmi suscettibili di recare danno
- R.B.2:** spamming o tecniche di sabotaggio
- R.B.3:** malfunzionamento, indisponibilità o degrado degli strumenti
- R.B.4:** accessi esterni non autorizzati
- R.B.5:** intercettazione di informazioni in rete
- R.B.6:** altro evento

- R.C.1:** accessi non autorizzati a locali/reparti ad accesso ristretto
- R.C.2:** sottrazione di strumenti contenenti dati
- R.C.3:** eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc.), nonché dolosi, accidentali o dovuti ad incuria
- R.C.4:** guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc);
- R.C.5:** errori umani nella gestione della sicurezza fisica

Si ricorda (cfr. quanto già esplicitato in tabella 1) che i rischi relativi agli strumenti sono stati oggetto di valutazione per la sola parte relativa ai trattamenti effettuati su sistemi propri (colonna 6.2 di tabella 1).



"CODICE DELLA PRIVACY – DPS DLGS 196/03"

Colonna 2 – supporto

Viene indicato se i dati sono raccolti in/su :

- F: File**
- D: Database**
- C: Cartaceo**
- M: Mail**

Colonna 3 - presenza del rischio

Colonna a risposta binaria:

- 1:** indica la **presenza** del rischio
- 0:** indica l'**assenza** del rischio;

Colonna 4 - Descrizione dell'impatto sulla sicurezza in ragione della gravità

Descrive le possibili conseguenze dell'impatto e deve essere coordinato con le successive per la sua misurazione

Colonna 5 - gravità dell'evento

Descrive l'impatto sulla sicurezza in ragione della sua potenziale gravità, dove:

- 1:** indica un **livello basso**
- 2:** indica un **livello medio**
- 3:** indica un **livello elevato**

Colonna 6 – Probabilità dell'evento

Indica il grado di probabilità dell'accadimento, dove:

- 1:** indica un **livello basso**
- 2:** indica un **livello medio**
- 3:** indica un **livello elevato**

Occorre precisare che nella valutazione del grado di probabilità dell'evento si è tenuto conto delle misure già adottate per fronteggiarlo; dette misure, ove non espressamente specificate nella stessa colonna , sono esplicitate nella successiva tabella 4



Istruzioni relative alla tabella 4 – Misure in essere e da adottare per contrastarli (reg. 19.4)

Contenuti

Vengono riportate, in forma sintetica, le misure in essere e da adottare per contrastare i rischi individuati.

Per misura si intende lo specifico intervento tecnico od organizzativo posto in essere per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia, come pure quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia.

Informazioni essenziali

Colonna 1 - Misure

La colonna indica con la lettera M seguita dal numero relativo alla misura sotto riportata, secondo l'elenco fornito dall'All. B (disciplinare tecnico in materia di misura di sicurezza) al D. Lgs. 196/2003 adottate per combattere i rischi riportati nella tabella 3. La numerazione non è necessariamente coincidente con quella del citato allegato B in ragione della mancata indicazione della misura 19 dello stesso, la prova della cui adozione è fornita peraltro dalla stesura del presente documento.

- 1) Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
- 2) Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
- 3) Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
- 4) Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
- 5) La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
- 6) Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
- 7) Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
- 8) Le credenziali sono disattivate anche in caso di perdita della qualifica che consente all'incaricato l'accesso ai dati personali.



"CODICE DELLA PRIVACY – DPS DLGS 196/03"

- 9) Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
- 10) Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
- 11) Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.
- 12) Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
- 13) I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
- 14) Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.
- 15) Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
- 16) I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
- 17) Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
- 18) Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.
- 19) I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
- 20) Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
- 21) I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
- 22) Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.



"CODICE DELLA PRIVACY – DPS DLGS 196/03"

- 23) Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.
- 24) Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che attesta la conformità alle disposizioni del presente disciplinare tecnico
- 25) Il titolare riferisce, nella relazione accompagnatoria al bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.
- 26) Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
- 27) Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
- 28) L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate. Si ricorda che:
le misure da 1 a 25 riguardano trattamenti effettuati con strumenti elettronici;
le misure da 26 a 28 riguardano trattamenti effettuati senza l'ausilio di strumenti elettronici;
le misure da 19 a 23 riguardano trattamenti di dati sensibili o giudiziari.
A dette misure se ne aggiungono altre, non comprese nel citato allegato B, che vengono indicate di seguito, con ripresa della precedente numerazione progressiva.
- 29) Sono stati adottati sistemi di registrazione degli accessi e uscite dei dipendenti, di somministrati, di clienti, fornitori e più in generale di chiunque acceda all'azienda
- 30) Esistono sistemi e dispositivi antincendio (estintori, manichette, impianti di rilevazione e/o spegnimento automatico)
- 31) Vengono utilizzati armadi muniti di chiavi e classificatori non accessibili
- 32) I locali aziendali sono dotati di dispositivi antintrusione (*).
- 33) L'azienda è dotata di adeguati sistemi di chiusura dei locali.
- 34) Aumentare il numero di sistemi in cluster



"CODICE DELLA PRIVACY – DPS DLGS 196/03"

- 35) E' in fase di valutazione circa la coerenza con le nuove indicazioni emesse dal garante privacy a tutela del personale dipendente, l'opportunità di tracciamento delle operazioni effettuate, con la registrazione di: epoca dell'operazione, indirizzo di rete della postazione accedente, descrizione dell'operazione eseguita. I file di log saranno accuratamente conservati per l'eventuale controllo.
- 36) Sta per essere adottato un sistema anti-intrusione (Intrusion Prevention System) in grado di individuare, tracciare e bloccare i tentativi di attacco già noti. Le regole di controllo sono verificate con regolarità dal fornitore dell'apparato. I file di tracciamento di tali tentativi sono controllati con regolarità dagli amministratori del sistema.
- 37) Sono in corso di revisione i regolamenti aziendali, al fine di predisporre un testo unico delle normative in materia di privacy, utilizzo di internet e posta elettronica da parte del personale dipendente, alla luce delle indicazioni recentemente fornite dal Garante privacy.

Occorre ricordare, infine che, mentre le misure relative a rischi derivanti da comportamenti degli operatori e da eventi relativi al contesto (colonna 1.1 di tabella 3) riguardano l'interezza dei trattamenti, le misure relative agli eventi relativi agli strumenti (sempre colonna 1.1 di tabella 3) si applicano ai soli trattamenti di cui Energie Locali S.r.l. sia Titolare (lettera T di colonna 1.2 di tabella 1)

Colonna 2 – descrizione dei rischi contrastati

Riporta, attraverso il relativo codice numerico il tipo di rischio contrastato, coerentemente a quelli indicati in colonna 1 della tabella 3 i rischi contrastati;

Colonna 3 – trattamenti interessati

Riporta, sulla base della classificazione adottata in colonna 6.3 di tabella 1, il supporto sul quale i trattamenti sono gestiti.

Tutti i trattamenti gestiti su quel supporto sono interessati adozione della misura.

Per comodità si riporta la legenda di colonna 6.3 di tabella 1:

F: File
D: Database
C: Cartaceo
M: Mail

Colonna 4 – misura già in essere

Il numero 1 indica l'avvenuta adozione della misura.

Colonna 4 – misura da adottare

Il numero 1 indica che la misura è ancora da adottare

Colonna 5 – struttura o persone addette all'adozione

La competenza delle strutture interne viene indicata attraverso il ricorso ai codici di cui alla colonna 5 della tabella 1, che, per comodità si riportano:

DG: Direzione Generale
DC: Direzione Commerciale
AT: Assistenza Tecnica
OUT: Outsourcer



Istruzioni relative alla tabella 5 – Criteri e modalità di ripristino della disponibilità dei dati (reg. 19.5)

Contenuti

Sono descritti i criteri e le procedure adottati per il ripristino dei dati in caso di loro danneggiamento o di inaffidabilità della base dati.

L'importanza di queste attività deriva dall'eccezionalità delle situazioni in cui il ripristino ha luogo: è essenziale che, quando necessarie, le copie dei dati siano disponibili e che le procedure di re installazione siano efficaci.

Si procede pertanto anche ad una sintetica descrizione dei criteri e delle procedure adottate per il salvataggio dei dati al fine di una corretta esecuzione del loro ripristino

Informazioni essenziali

Colonna 1- supporto elettronico utilizzato per il trattamento dei dati

Indica il supporto (archivio) elettronico nel quale vengono raccolti i dati:

F: File

D: Database

Tutti i trattamenti effettuati su quel tipo di supporto hanno criteri e modalità di ripristino comuni.

Colonna 3 -back up

Indica la frequenza dei back up

Colonna 4- Criteri e procedure per il salvataggio e il ripristino dei dati

Indica sinteticamente criteri e procedure utilizzate per il salvataggio ed il ripristino dei dati

Colonna 5- pianificazione delle prove di ripristino

Indica sinteticamente criteri le tempistiche (delle prove) di il ripristino dei dati



Istruzioni relative alla tabella 6 – Pianificazione degli interventi formativi (reg. 19.6)

Contenuti

Vengono riportate le informazioni necessarie per individuare il quadro sintetico degli interventi formativi che si prevede di svolgere

Informazioni essenziali

Colonna 1- Descrizione sintetica degli interventi formativi

Vengono indicati gli interventi formativi effettuati e da effettuarsi

Colonna 2 - Classi di incarico o tipologie di incaricati interessati

Vengono dettagliati i destinatari degli interventi formativi in funzione della posizione aziendale, distinguendo tra:

- R** responsabili di strutture aziendali;
- C** responsabili/coordinatori di servizi;
- OS** operatori su dati sensibili/giudiziari
- ALL** tutti coloro che trattano dati personali

Colonna 3 - Tempi previsti

Si procede all'indicazione dei tempi di attuazione degli interventi formativi, individuando alternativamente:

- una data limite specificamente indicata;
- un termine legato ad un evento, di cui viene specificato il nome, seguito dal numero massimo di giorni entro i quali l'intervento formativo deve essere realizzato;
- in caso di attività di rinforzo/aggiornamento, la frequenza minima con cui detta attività deve essere svolta (ad esempio: una volta l'anno)



Istruzioni relative alla tabella 7 – Trattamenti affidati all'esterno (reg. 19.7)

Contenuti

Viene redatto un quadro sintetico delle attività affidate a terzi che comportano il trattamento di dati, con l'indicazione sintetica del quadro giuridico o contrattuale (nonché tecnico e organizzativo) in cui tale trasferimento si inserisce, in riferimento agli impegni assunti, anche all'esterno, per garantire la protezione dei dati stessi.

Informazioni essenziali

Si precisa preliminarmente che in questa tabella non compaiono, oltreché ovviamente i trattamenti integralmente svolti internamente da Energie Locali S.r.l., anche i trattamenti, indicati in tabella 1 colonna 1.2 con la lettera R (Responsabile), che possono essere compiuti da soggetti titolari di quel trattamento e cioè committenti (o committenti di committenti) di Energie Locali S.r.l. (soggetti identificati con i codici C1 e C2 nelle colonne 2.2 e 5 della tabella 1).

Colonna 1- identificativo del trattamento

Numero progressivo utilizzato nella colonna 1.1. della tabella 1

Colonna 2- Descrizione sintetica della finalità perseguita/attività svolta

Corrisponde alla colonna 2 di tabella 1

Si articola in una colonna 2.1 nella quale viene riportato un codice che corrisponde all'attività svolta, ed in una colonna 2.2 nella quale viene riportato un codice relativo alle categorie di interessati.

La legenda dei codici effettivamente utilizzati vengono riportate di seguito.

PACO: Paghe e Contributi

Procedere all'elaborazione delle buste paga per dipendenti e collaboratori, e dare corso ai conseguenti adempimenti assistenziali, previdenziali e fiscali

M626: Medico 626

Esercitare la sorveglianza sanitaria prevista dal D. Lgs. 626/1994

Colonna 2.1

DS: Dipendenti/Somministrati

DC: Dipendenti/collaboratori

Colonna 3 - Natura dei dati trattati

La colonna è stata distinta in relazione al trattamento di dati sensibili (3.1) e giudiziari (3.2).

In entrambe le colonne il numero 1 indica la presenza di dati di tale natura, il numero 0 l'assenza degli stessi.

Colonna 4 – soggetto esterno

Si procede all'indicazione del soggetto esterno

Colonna 5 – ruolo del soggetto esterno



"CODICE DELLA PRIVACY – DPS DLGS 196/03"

Nella colonna viene indicato se il soggetto è:

T: Titolare del trattamento

R: Responsabile del trattamento

Colonna 6 – descrizione dei criteri

Viene specificato quale dei seguenti impegni è stato assunto, con specifiche dichiarazioni/documenti oppure su base contrattuale :

1. trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto;
2. adempimento degli obblighi previsti dal Codice per la protezione dei dati personali;
3. rispetto delle istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o integrazione delle procedure già in essere;
4. impegno a relazionare periodicamente sulle misure di sicurezza adottate – anche mediante eventuali questionari e liste di controllo – e ad informare immediatamente il titolare del trattamento in caso di situazioni anomale o di emergenze.



"CODICE DELLA PRIVACY – DPS DLGS 196/03"

ALLEGATI AL DOCUMENTO

- Tabella 1: Elenco trattamento dei dati personali
- Tabella 2: Distribuzione dei compiti e delle responsabilità
- Tabella 3: Analisi dei rischi che incombono sui dati
- Tabella 4: Misure in essere e da adottare per contrastarli
- Tabella 5: Criteri e modalità di ripristino della disponibilità dei dati
- Tabella 6: Pianificazione degli interventi formativi
- Tabella 7: Trattamenti affidati all'esterno
- Schema Rete