

Allegato H1

Gent. NOME E COGNOME INCARICATO

RIF. CONTRATTO N..... TRA ENEL X ITALIA S.P.A. E PARTNER

DATA DI SOTTOSCRIZIONE DEL CONTRATTO .../.../.....

DURATA DEL CONTRATTO DA/...../..... A/...../.....

Oggetto: DESIGNAZIONE AD "INCARICATO DEL TRATTAMENTO DEI DATI"- ART. 30, CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (D.LGS. N. 196 DEL 30 GIUGNO 2003)

La Società, in qualità di Responsabile del trattamento dei dati personali nella titolarità di Enel X Italia trattati in forza del Contratto di cui sopra

PREMESSO CHE

- Lo svolgimento delle attività inerenti la Sua mansione/qualifica contrattuale implica il trattamento di dati personali e richiede, tra l'altro, in relazione al Contratto citato, l'accesso ai sistemi informatici della Società Enel X Italia S.p.A., Titolare del trattamento dei dati personali;
- A tal fine è necessaria la Sua abilitazione ai predetti sistemi;
- Il trattamento menzionato e la suddetta abilitazione presuppongono la Sua designazione ad Incaricato al trattamento, ai sensi dell'art. 30, Codice privacy;

TUTTO CIÒ PREMESSO

la scrivente Società

INCARICA

il Sig., nato a il
C.F., al trattamento dei dati personali, cioè a qualsiasi operazione, anche di mera consultazione, relativa a dati personali (inseriti in archivi informatici e/o cartacei detenuti dalla scrivente Società e/o dalla Società Enel X Italia S.p.A., Titolare del trattamento) connessa allo svolgimento delle funzioni relative alla Sua mansione/qualifica....., presso la sede di

In particolare il predetto trattamento è finalizzato allo svolgimento di:

- Attività di vendita di prodotti e servizi in favore di cliente di Enel X Italia o di clienti potenziali; gestione richieste di clienti di Enel X Italia, successive alla sottoscrizione di un contratto, come meglio ivi specificate;

Vengono di seguito fornite informazioni ed istruzioni minime volte all'assolvimento dei compiti a Lei assegnati in relazione alle operazioni di trattamento di dati personali.

In particolare, si precisa che:

- Il trattamento dei dati personali deve essere effettuato in modo lecito e corretto;
- I dati personali devono essere raccolti e registrati unicamente per finalità connesse all'attività svolta, esclusivamente negli orari di lavoro e comunque non oltre il tempo necessario;

- Fatto salvo quanto sopra, nell'eccezionale ipotesi di trattamento dei dati personali svolto fuori dall'orario di lavoro, l'Incaricato deve accertarsi di aver chiuso la sessione di lavoro ("log-off") in modo che siano richieste le credenziali di accesso al successivo utilizzo;
- È necessaria la verifica costante dei dati ed il loro aggiornamento;
- È necessaria la verifica costante della completezza e pertinenza dei dati trattati;
- La eventuale fase di raccolta del consenso deve essere preceduta da apposita informativa e dal rilascio del consenso degli interessati, che deve essere libero, specifico e in forma scritta o comunque appositamente documentata;
- In caso di interruzione, anche temporanea, del lavoro è necessario assicurarsi che i dati trattati non siano accessibili a terzi non autorizzati, effettuando apposito log-off;
- Le proprie credenziali di autenticazione dovranno essere riservate e in quanto tali utilizzate unicamente dal soggetto designato Incaricato;
- In ogni operazione di trattamento deve essere garantita la massima riservatezza. In particolare Lei è tenuto a:
 - non lasciare incustoditi o esposti alla visione di soggetti comunque estranei al trattamento i documenti, cartacei e/o elettronici, contenenti i dati oggetto di trattamento; curare la necessaria riservatezza dei dati in questione, mettendo in atto - anche sulla base delle disposizioni impartite dalla Società e/o dalle Società Titolari - le cautele idonee ad evitare che altri, non autorizzati, possano accedere ai suddetti dati;
 - non diffondere o comunicare i dati di cui è venuto in possesso, al di fuori dei casi consentiti dalla legge o previsti dalle norme contrattuali e mantenere il dovuto riserbo in ordine alle informazioni delle quali sia venuto a conoscenza nel corso dell'incarico anche quando sia venuto meno l'incarico stesso;
 - in ogni caso, custodire con cura e diligenza appropriata la documentazione cartacea e/o elettronica affidatale nello svolgimento dell'attività lavorativa e in particolare quella contenente dati sensibili e/o giudiziari, in armadi o cassette muniti di serratura e osservare la procedura eventualmente prevista (indicazione nell'apposito registro del proprio nominativo, orario e data di accesso, prelievo/restituzione del documento) per l'accesso agli archivi che conservano i dati sopra menzionati;
 - informare il Responsabile in caso di incidenti che coinvolgano i dati personali oggetto del trattamento, in particolare se sensibili e/o giudiziari.

In ogni caso sarà Sua cura attenersi scrupolosamente alle **prescrizioni dettate in materia di misure minime di sicurezza di cui all'Allegato B, Codice Privacy**, c.d. "Disciplinare tecnico in materia di misure minime di sicurezza", allegato alla presente e parte integrante della stessa, di cui Lei dichiara di avere preso visione, nonché di quelle ulteriori eventualmente dettate dalla scrivente Società e/o dalle Società Titolari, i cui eventuali aggiornamenti Le verranno comunicati.

Inoltre, premesso che:

Ai sensi del CONTRATTO N..... TRA ENEL X ITALIA S.P.A. E PARTNER:

- a. InfoCert e Enel X Italia hanno concluso una Convenzione denominata "Convenzione per lo svolgimento di attività di Ufficio di Registrazione e rilascio di servizi di certificazione digitale e della Carta Nazionale dei Servizi", in funzione della quale Enel X Italia è stata nominata "Ufficio di Registrazione";
- b. InfoCert, con separato atto, ai fini del rispetto della normativa privacy, ha designato Enel X Italia quale soggetto "Responsabile del Trattamento dei dati personali in esecuzione del mandato conferito con la Convenzione di cui alla lett. a), riconoscendole la facoltà di nominare soggetti, persone fisiche o giuridiche ("I.R.") al fine di svolgere parte delle attività di identificazione volte al rilascio dei servizi di certificazione digitale";
- c. Enel X Italia, con separato atto, ha provveduto a designare nel rispetto di quanto previsto dalla Convenzione di cui alla precedente lett. a), il Partner quale Sub-Contrattante e "Incaricato della Registrazione" ("IR"), al fine di delegare a quest'ultimo lo svolgimento di una parte delle attività dell'Ufficio di Registrazione;
- d. nello svolgimento delle attività ad esso delegate, l'IR è ammesso ad avvalersi di persone fisiche preposte alla realizzazione delle attività di identificazione per conto dell'Ufficio di Registrazione (di seguito, "Addetti/o");

tutto ciò premesso

il Partner, quale Sub-contraente a tal fine nominato da Enel X Italia limitatamente alle attività volte al rilascio dei servizi di certificazione digitale designa i soggetti che operano per proprio conto quali "Incaricati al trattamento dei dati personali in esecuzione del mandato conferito con la Convenzione di cui alla lett. a)";

Con riferimento alle attività di registrazione e rilascio di servizi di certificazione digitale, l'Incaricato compirà le operazioni di trattamento dei dati personali, secondo quanto previsto nel Manuale Informativo allegato al Contratto nonché secondo le istruzioni impartite da InfoCert nel corso della formazione ricevuta, che varia in base alla procedura di identificazione messa in atto. In particolare, l'Incaricato metterà in atto le seguenti operazioni di trattamento:

- verifica del documento di identità del richiedente, della relativa validità e della corrispondenza al soggetto richiedente;
- trascrizione o verifica (in base alle indicazioni fornite in sede di formazione) delle informazioni inerenti la persona fisica richiedente;
- produzione della documentazione che attesta l'avvenuto riconoscimento del richiedente;
- raccolta dei documenti firmati, se applicabile sulla base della procedura di identificazione messa in atto.

Si rileva infine quanto segue:

- la presente lettera di designazione cesserà di produrre effetti alla data di cessazione del rapporto di lavoro o dell'incarico con la Scrivente società; successivamente a detta data, pertanto, ogni trattamento dei dati personali, incluso l'accesso ai sistemi informatici della Scrivente Società e/o delle Società Titolari, è vietato e sanzionato secondo le vigenti disposizioni di legge (cfr. a mero titolo esemplificativo l'art. 615-ter, codice penale su "Accesso abusivo ad un sistema informatico o telematico");
- copia della presente lettera sarà restituita dall'Incaricato alla Scrivente Società, sottoscritta per conoscenza ed accettazione, sarà conservata dalla medesima Società e da quest'ultima messa a disposizione delle Società Titolari sua espressa richiesta, entro e non oltre due giorni dalla richiesta stessa;
- per evitare trattamenti dati non autorizzati sarà cura della Scrivente Società informare le Società Titolari della interruzione del rapporto di lavoro o dell'incarico in essere entro e non oltre due giorni dall'evento, al fine di consentire alle Società Titolari di disporre la revoca immediata delle abilitazioni informatiche dalla stessa rilasciate.

_____,/...../.....

Il Responsabile del Trattamento Dati

Per conoscenza e presa visione

l'Incaricato del trattamento

**Istruzioni di cui al
Decreto Legislativo 30 giugno 2003, n. 196
Codice in materia di protezione dei dati personali
Disciplinare Tecnico sub All. B)**

Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

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 qualità che consente all'incaricato l'accesso ai dati personali.
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.

Sistema di autorizzazione

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.

Altre misure di sicurezza

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.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

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.

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.

Misure di tutela e garanzia

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 ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

Trattamenti senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

25. 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.

26. 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.

27. 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.